SSH Secure Shell for Workstations Windows Client Version 3.1 User Manual

November, 2001

SSH Communications Security Corp.
Fredrikinkatu 42
FIN-00100 Helsinki
FINLAND

SSH Communications Security Inc.
1076 East Meadow Circle
Palo Alto, CA 94303
USA

SSH Communications Security K.K.
House Hamamatsu-cho Bldg. 5F
2-7-1 Hamamatsu-cho, Minato-ku
Tokyo 105-0013, JAPAN

http://www.ssh.com/
e-mail: ssh-sales@ssh.com (sales), http://www.ssh.com/support/ssh/ (support)
Tel: +358 20 500 7030 (Finland), +1 650 251 2700 (USA), +81 3 3459 6830 (Japan)
Fax: +358 20 500 7031 (Finland), +1 650 251 2701 (USA), +81 3 3459 6825 (Japan)

Contents

Chapter 1

Introduction

The SSH Secure Shell for Workstations Windows client (ssh2 client) is a program that allows secure network services over an insecure network.

SSH Secure Shell for Workstations Windows Client replaces other, insecure terminal applications, such as Telnet and FTP. It allows you to securely login to remote host computers, to execute commands safely on a remote computer, and to provide secure encrypted and authenticated communications between two hosts in an untrusted network. X11 connections and arbitrary TCP/IP ports can also be forwarded over the secure channel, expanding SSH Secure Shell's usability even further.

SSH Secure Shell with its array of unmatched security features is an essential tool for today's network environment. It is a powerful guardian against the numerous security hazards that threaten network communications.

1.1 Network Security Risks

The open architecture of Internet Protocol (IP) makes it a highly efficient, cost-effective, and flexible communications protocol for local and global communications. It has been widely adopted, not only on the global Internet, but also on the internal networks of large corporations.

Internet Protocol was designed to be highly reliable against random network errors. However, it was not designed to be secure against a malicious attacker. In fact, it is vulnerable to a number of well-known attacks. This is preventing it from being used to its fullest for business and other purposes involving confidential or mission-critical data.

1.1.1 Security of Internet Protocol

The IP protocol suite, including TCP/IP, was designed to provide reliable and scalable communications over real-world networks. It has served this goal well. However, it was designed twenty years ago in a world where the Internet consisted of a few hundred closely controlled hosts. The situation has changed. The Internet now connects tens of millions of computers, controlled by millions of individuals and organizations. The core network itself is administered by thousands of competing operators, and the network spans the whole globe, connected by fibers, leased lines, dialup modems, and mobile phones.

The phenomenal growth of the Internet has peaked the interest of businesses, military organizations, governments, and criminals. Suddenly, networks are changing the way business is done. They have changed the nature of trade and distribution networks, and the way individual people communicate with each other.

This upsurge of business communications, scientific communications and political communications on the Internet has also brought out negative elements. Criminals are looking for ways of getting a cut of the emerging business. Industrial espionage has become a reality. Intelligence agencies are showing growing interest towards networked communications, and they often exchange information with domestic commercial interest and political groups. Crackers, exchanging information and source code, make attacks that ten years ago were thought to be only within the reach of superpowers' intelligence agencies.

Consequently, the IP protocol, while very tolerant of random errors, is vulnerable to malicious attacks. The most common types of attacks include:

- Eavesdropping on a transmission, for example, looking for passwords, credit card numbers, or business secrets.
- Hijacking, or taking over a communication in such a way that the attacker can inspect and modify any data being transmitted between the communicating parties.
- IP spoofing, or faking network addresses or host names in order to fool access control mechanisms based on them or to redirect connections to a fake server.

The ssh2 protocol is designed to protect network communications against security hazards like these.

1.2 Different SSH Versions

Several different Secure Shell client and server versions exist. The different versions use different implementations of the SSH protocol.

SSH Secure Shell for Workstations Windows client uses SSH protocol version 2 (ssh2), but also supports connections to SSH version 1 (ssh1) servers. Note, however, that SSH version 2 (ssh2) is a more advanced protocol than the legacy version ssh1. For more information on the implications of using an ssh1 connection, see the SSH web site `http://www.ssh.com/products/ssh/advisories/statement.cfm`.

Note: SSH Communications Security has deprecated the ssh1 protocol and does not recommend using it. For more information, see `http://www.ssh.com/products/ssh/cert/deprecation.cfm`.

The ssh2 protocol provides a set of radical improvements to ssh1. These improvements include:

- A much better understood and more secure protocol.
- A new design which requires much less code to be run with administrative privileges.
- Totally rewritten code that improves security.
- New routines for cryptography and mathematics, resulting in considerable improvements in speed.
- Support for multiple public key algorithms, including RSA, DSA and Diffie-Hellman key exchange.
- Easy to use file transfers using the integrated file transfer agent in SSH Secure Shell for Workstation Windows client, and the scp2 (secure file copy) and sftp2 (secure file transfer protocol) command line applications.

1.3 SSH2 Protocol Features

The ssh2 protocol contains the following features:

- Secure terminal sessions utilizing secure encryption.
- Full, secure replacement for FTP and Telnet, as well as the UNIX r-series of commands: `rlogin`, `rsh`, `rcp`, `rexec`.
- Multiple high security algorithms and strong authentication methods that prevent such security threats as identity spoofing and man-in-the-middle attacks.
- Multiple ciphers for encryption, including e.g. 3DES, Blowfish and AES.
- Password, public key, certificate, smart card, PAM and SecurID authentication methods.
- Transparent and automatic tunneling of X11 connections and arbitrary TCP/IP-based applications, such as e-mail.
- Automatic and secure authentication of both ends of connection. Both the server and the client are authenticated to prevent identity spoofing, Trojan horses, etc.
- Unique secure file transfer interface (SFTP) fully integrated in the client software.
- Multiple channels that allow you to have multiple terminal windows and file transfers going through one secure and authenticated connection.

1.4 New Features

This version of SSH Secure Shell for Workstation Windows client contains several new features and enhancements.

Some of the most notable new features of SSH Secure Shell version 3.1 are the following:

File transfer speed increase

Files can now be transferred significantly faster.

Keymap editor

The integrated keymap editor makes it easy to change the assigned keyboard keys to suit your personal preferences.

Paste selection on right mouse click

Now you can copy text on the terminal window simply by highlighting it with the mouse and then paste it by clicking the right mouse button.

SSH Accession support

Support for SSH Accession makes public-key authentication a fast and automatic process.

Support for authentication agent forwarding

Authentication agent can automatize the use of authentication private keys. Agent forwarding can now be enabled or disabled based on the ssh protocol used.

URL capture

Now Internet addresses displayed on the terminal window function as links that can be activated with a mouse click.

User confirmation dialog customization

Now confirmation dialogs can have a preset response, so that the need for user confirmation on confirmation dialogs can be eliminated.

Various bug fixes

This version also contains fixes for various minor bugs found in previous releases.

1.5 System Requirements

The SSH Secure Shell for Workstation Windows client does not have any special hardware or software requirements. Any computer capable of running a current version of the Microsoft Windows operating system (Windows 95, Windows 98, Windows ME, Windows NT, or Windows 2000) and equipped with a functional connection to a remote host computer can be used.

The SSH Secure Shell for Workstations Windows client installation requires about 4 megabytes of disk space. Note that ssh2 will save each user's settings in that particular user's personal directory.

1.6 Desktop Icons

When you have installed the SSH Secure Shell for Workstations Windows client, you will have two separate program icons on the Windows desktop as well as in the Start menu (by default under **Start -> Programs -> SSH Secure Shell**).

The SSH Secure Shell Client icon and the SSH Secure File Transfer Client icon both start the same application, SSH Secure Shell for Workstations Windows client. The difference between the icons is that they use different settings files. The Secure Shell Client icon uses a settings file called `default.ssh2`, and the Secure File Transfer icon uses a settings file called `defaultsftp.ssh2`.

By default the settings files have been configured so that they open the appropriate SSH Secure Shell for Workstations window, either the terminal window or the SSH Secure File Transfer window. If you want to change the default configuration, you can save your settings to either a new settings file (using the Save As option from the File menu), or save the new settings using the old settings files (using the Save option from the File menu).

Please note that when you save your current settings, the window positions are also saved. If you open the SSH Secure File Transfer client by clicking the appropriate icon, then open a terminal window or two, and then save the settings, the 'extra' terminal windows will appear the next time you click the SSH Secure File Transfer Client icon. If you then close the File Transfer window and save your settings again, the next time you will see no File Transfer window at all.

Do not be alarmed by this - you can always open a new terminal or File Transfer window by clicking the appropriate toolbar button or selecting the appropriate menu item. If you then save your settings again, the new window positions will be used as default values for new connections.

For more information saving the current settings, see section 2.1 (Saving Settings).

1.7 Support

The most current version of the SSH Secure Shell for Workstations Windows client online help is available on the SSH Web pages: `http://www.ssh.com/products/ssh/winhelp/`.

Frequently asked questions specific to the SSH Secure Shell Windows client are answered in the SSH Secure Shell FAQ: `http://www.ssh.com/faq`.

If the product documentation and the FAQ do not answer your questions and you have purchased the software, you can contact SSH Secure Shell Technical Support. Use the online support form available at `http://www.ssh.com/support/ssh` for support requests and `http://www.ssh.com/support/ssh/bug-report.cfm` for bug reports.

Please see the SSH Web site (`http://www.ssh.com/support/ssh/support_offering.cfm`) for more information on the terms and conditions of obtaining technical support for SSH Secure Shell from SSH Communications Security.

Chapter 2

Configuration

Before establishing a connection to a remote host computer, you should first check your connection settings. The connection settings can be changed by using the Profiles option of the profiles toolbar (see section 3.2 (Profiles)), or alternatively by using the Settings option (see section 6.13 (Settings), found on the toolbar and the Edit menu).

The Profiles dialog can be used to configure the profile settings that are associated with a single remote host computer. With the Settings dialog you can control also the global settings that affect all connections.

To open the Settings dialog, click the Settings button on the toolbar or select the Settings option from the Edit menu.

The different settings categories are visible on the left hand side of the Settings window as a tree structure. Branches that have a plus sign (+) next to them can be expanded by clicking on the plus sign. Branches that have a minus sign (-) next to them can be collapsed by clicking on the minus sign.

Click on a branch to display the settings associated with it. You can change the settings by changing the selections displayed on the right hand side of the settings window. Note that some of the settings do not take effect until you save the settings and then open a new terminal or file transfer window, or start a new connection.

2.1 Saving Settings

When you have changed the settings, an asterisk (*) is displayed on the SSH Secure Shell for Workstations Windows client title bar, after the name of the current settings file (for example: `default*`). This indicates that the changed settings are not yet permanent - they have not been saved yet.

If you want to make the changes permanent, you can save them for later use. Click the Save button on the toolbar, or select the Save Setings menu option from the File menu to save any changes you have made to your current settings. The changes will be saved in the default settings file, `default.ssh2`.

The default settings file is loaded automatically when you start the SSH Secure Shell client. Therefore all the settings that you save in the default settings file take effect immediately when you run the ssh2 client. These settings are also used for connections started with the Quick Connect option (see section 3.1 (Quick Connect)).

Note that when you save the current settings, the positions of the currently open terminal and file transfer windows are also saved. If you arrange your window positions to suit your own taste and save the settings in the default settings file, the windows will be automatically positioned the way you prefere when you next run the SSH Secure Shell client.

If you spend a lot of effort customizing your own settings, it is a good idea to create backup copies of your customized settings files (`*.ssh2`) and store them in a safe location. This way you will not have to create the custom settings again, if for some reason (such as hardware failure) your settings files are lost.

2.2 Multiple Settings Files

You can save separate settings files for each remote host computer. This can be done by using the Profiles option. For more information on using profiles, see section 3.2 (Profiles).

2.3 Loading Settings

It is easy to use a profile that has been previously saved. Select the Profiles option (from the Profiles toolbar or the File menu), and you will see a menu of previously saved profiles. Click on a profile, and a connection using the profile settings will immediately be started.

Note that this also works when you are already connected to a remote host computer. The profile will start a new, separate connection.

Another way to load the settings for a particular connection is to double-click the settings file name, for example in Windows Explorer. When the SSH Secure Shell for Workstations Windows client is installed, files with the extension .ssh2 are associated with the SSH Secure Shell client. This means that you can start the SSH Secure Shell for Workstations Windows client with any settings file loaded by just doubleclicking on that settings file.

If you regularly connect to several remote host computers, you can create shortcuts to the corresponding settings files for example on the Windows desktop. This way you can quickly open the desired connection with the relevant settings already defined, just by clicking on an icon on the desktop.

2.4 Profile Settings

With the Profile Settings page of the Settings dialog you can configure separate connection settings for each particular remote host computer. To display the Profile Settings, open the Settings dialog and click on the Profile Settings text on the left hand side of the dialog.

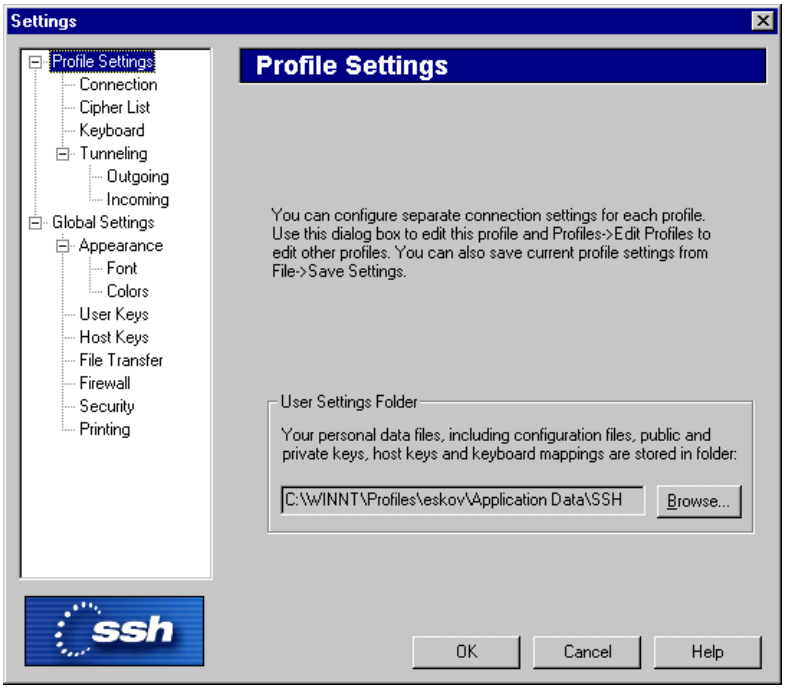

Figure 2.1: The Profile Settings page of the Settings dialog.

User Settings Folder

The directory path to your personal data files is displayed in the text field next to the Browse button. Note that this is not an editable field, but the location of these files can be set by defining the `SSHCLIENT_USERPROFILE` environment variable. For more information, see the SSH Secure Shell FAQ (`http://www.ssh.com/faq/`).

Your personal files include the settings file (default name default.ssh2), your public and private keys, host keys and the keyboard mapping file (KEYMAP.MAP).

Click the Browse button to quickly access your personal data files. The folder where the settings files are saved will open. This is useful if you wish to copy or backup your personal settings.

Note that your private keys should always be kept secret. This is important to remember if you are sharing your local computer with other users. In such case, it is not advisable to store your private keys on the local disk. For more information on user key files, see section 3.6 (Using Public-Key Authentication).

OK

Click the OK button to start using the specified settings.

Cancel

Click the Cancel button to abort any changes you have made to the settings.

Help

Click the Help button to see the relevant help section.

2.4.1 Connection

The protocol settings used in the connection are configured using the Connection page of the Settings dialog. Any changed connection settings will take effect the next time you login.

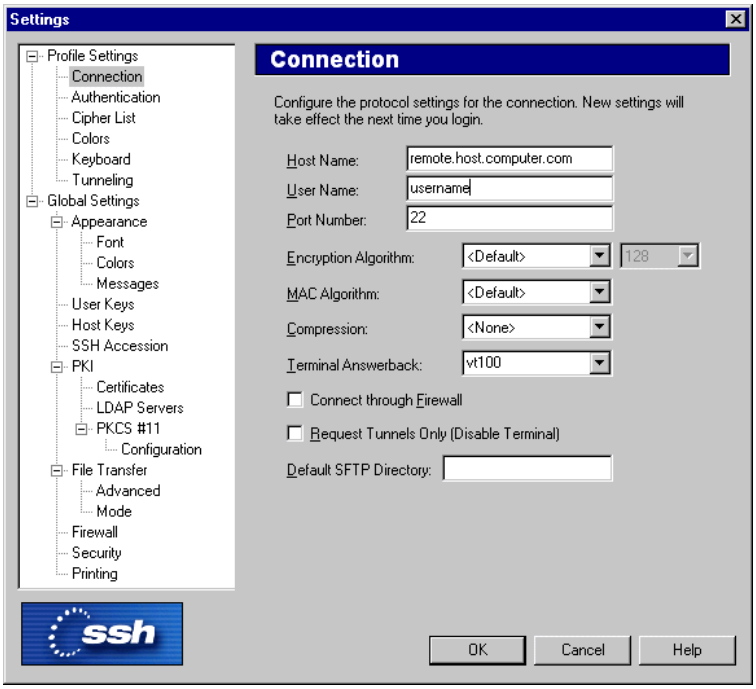

Figure 2.2: The Connection page of the Settings dialog.

Host Name

Type the name of the remote host computer which you will connect to using this profile.

User Name

Type the user name you want to use when connecting to the remote host computer.

Port Number

Type the port number you want to use for the ssh2 connection. The default port is 22.

Note: that an `sshd2` daemon program must be listening on the specified port on the remote host computer or the connection attempt will not succeed. If you are unsure of which port the remote host computer is listening to, contact the system administrator of the remote host.

Encryption Algorithm

Select the desired encryption algorithm from the dropdown menu. Valid choices are `3DES`, `Blowfish`, `Twofish`, `AES`, `Arcfour`, and `CAST`. You can also select whatever `default` that is used by the remote host computer, use no enryption (`none`) at all, or create your own customized `cipher list`. For more information on the `Cipher List` option, see section 2.4.3 (Cipher List).

For the AES and Twofish algorithms you can also choose the strength of encryption, ie. how many bits will be used. Greater values are more secure, but slower to use. Possible values are 128, 192 or 256 bits.

Note: If you select `none` as the encryption algorithm, the communications for this profile will not be encrypted and all information will be sent as plaintext. The `none` encryption method is not secure and is not recommended. Use it only if you are sure of what you are doing. A warning dialog will be displayed, if you select this option.

MAC Algorithm

Select the desired Message Authentication Code (MAC) algorithm (hash algorithm) from the dropdown menu. Valid choices are `HMAC-MD5` and `HMAC-SHA1`. You can also select whatever `default` that is used by the remote host computer, or select to use no message authentication code at all (`none`). If you select not to use any MAC algorithm, a confirmation dialog will be displayed.

Compression

Select the desired compression setting from the dropdown menu. Valid choices are zlib and none.

Terminal Answerback

Select the desired terminal answerback from the dropdown menu. Possible choices are ansi, vt100, vt102, vt220, vt320 and xterm.

Connect through Firewall

Check the check box if you are connecting through a firewall. For more information on the firewall settings, see section 2.5.18 (Firewall).

Request Tunnels Only (Disable Terminal)

Check the Request Tunnels Only check box if you wish to only set up the specified tunnels and not request a terminal or file transfer session.

Default SFTP Directory

Type the path to the directory that you want to use as the default local directory for Secure File Transfer operations.

2.4.2 Authentication

With the Authentication page of the Settings dialog, you can define customized authentication methods. Two lists are displayed on the page, the upper list for general authentication, and the lower list for authentication methods user for public-key authentication.

The icons displayed above the list can be used to add a new authentication method, delete an existing authentication method and move the authentication methods upwards or downwards in the preference list. Authentication methods higher up in the list will be attempted first.

Figure 2.3: Defining the authentication settings

Possible methods for general authentication are the following:

Password

Use password for authentication.

Public Key

Use public-key authentication.

SecurID

Use SecurID for authentication. Using SecurID authentication requires that you have a SecurID device that generates the numeric codes that are needed to login.

PAM

Use Pluggable Authentication Modules (PAM) for authentication. PAM is an authentication method that has gained wide popularity especially on UNIX platforms.

Possible methods for public-key authentication are the following:

User Keys

Use user keys for authentication. For more information on using user keys, see section 2.5.5 (User Keys).

User Certificates

Use user certificates for authentication. For more information on using certificates, see section 2.5.9 (Certificates).

PKCS #11 Keys

Authenticate by using PKCS #11 keys (keys stored for example on a smart card). For more information on using PKCS #11 keys, see section 2.5.12 (PKCS 11).

PKCS #11 Certificates

Authenticate by using PKCS #11 certificates (certificates stored for example on a smart card). For more information on using PKCS #11 certificates, see section 2.5.12 (PKCS 11).

SSH Accession Keys

Use SSH Accession keys for authentication. SSH Accession is a separate software product by SSH Communications Security that offers an easy method for utilizing digital certificates and smart cards.

SSH Accession Certificates

Use SSH Accession for authentication. SSH Accession is a separate software product by SSH Communications Security that offers an easy method for utilizing digital certificates and smart cards.

Note: The automatically handled authentication methods should always be listed first, i.e. public-key authentication should preceed password authentication. This way the automatically handled method will be used whenever possible.

2.4.3 Cipher List

With the Cipher List page of the Settings dialog you can control which ciphers can be used for the connection. This selection defines what encryption methods will be available when using the `Cipher List` encryption algorithm setting.

The following algorithms can be selected:

AES128

AES192

AES256

3DES

Blowfish

CAST128

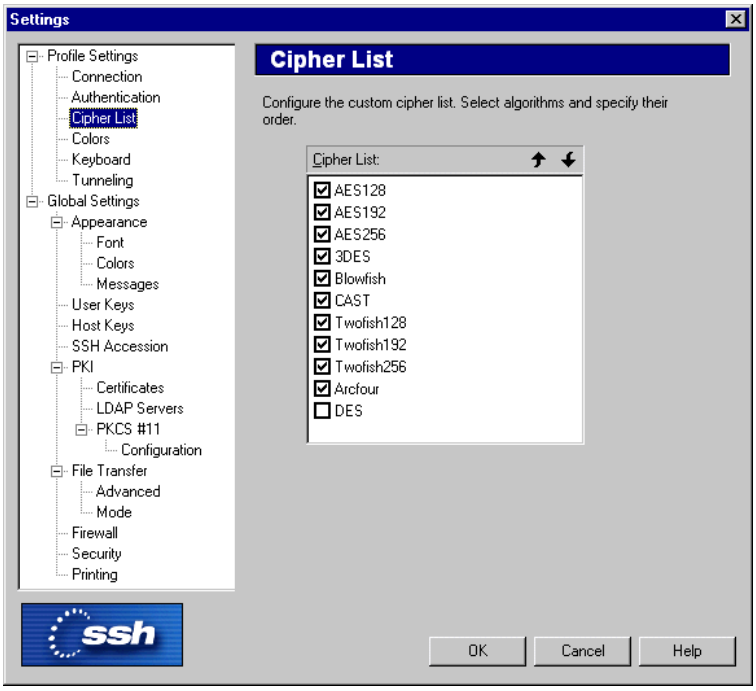

Figure 2.4: Select your preferred encryption algorithms with the Cipher List page.

Twofish128

Twofish192

Twofish256

Arcfour

DES

Please note that DES is a legacy cipher that is not considered to be cryptographically secure. DES is only included for compatibility with some older protocol versions. It is *strongly* recommended that DES is not used.

You can add new ciphers to the Cipher List and remove undesired ciphers from the list with the New and Delete buttons, and change their order of preference with the Up and Down buttons.

New

Click the New button (the leftmost button on the top right hand side of Cipher List) to add a new cipher to the list from a dropdown menu. The keyboard shortcut for the New button is the `Ins` key.

Delete

Select an unwanted cipher entry from the list and then click the Delete button (the second button on the top right hand side of the cipher list) to remove the cipher. The keyboard shortcut for the Delete button is the `Delete` key.

Up

You can give a cipher a higher priority by clicking it with the mouse, and then clicking the Up button. The marked algorithms that are located on the top of the list are preferred.

SSH Secure Shell will try to use the first marked algorithm in the connection. If that algorithm is not supported by the remote host computer, the client software will try the next marked algorithm on the list, and so on.

Down

To give a cipher a lower priority rating, select it with the mouse, and then click the Down button.

Click the check box next to each algorithm to include or exclude it in the list of available custom algorithms. An algorithm marked with a check mark is available for use.

To use your customized list of preferred encryption algorithms, select `Cipher List` as the encryption algorithm on the Connection page of the Settings dialog. For more information, see section 2.4.1 (Connection).

2.4.4 Colors

The colors used in the terminal window can be selected using the Colors page of the Settings dialog. The new color settings are active immediately when you click the OK button. Note that changing the terminal colors does not affect what is already visible on the terminal window, but the text output from this point onwards will use the set color scheme.

To discard the changes, click the Cancel button.

Use Global Colors

Select the Use Global Colors check box if you want to use the same color settings for each connection. If the check box is selected, you cannot specify different color settings for each connection profile (the other color settings are grayed out).

The Use Global Colors check box is visible only on the Colors page that is located under Profile Settings in the Settings dialog.

Text Colors

The text colors affect the terminal window background color and the color of text in both a connected window and a disconnected window.

Foreground

Select the desired foreground color from the dropdown menu. Foreground color is used for text in a window that has a connection to a remote host computer. Sixteen colors are available for your selection. Black is the default foreground color.

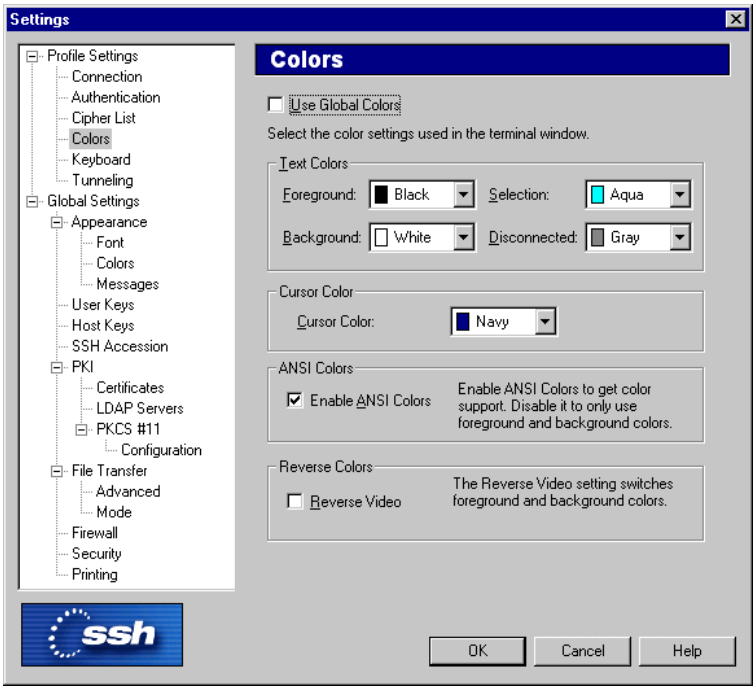

Figure 2.5: The Colors page of the Settings dialog.

Background

Select the desired background color from the dropdown menu. Sixteen colors are available for your selection. White is the default background color.

Selection

Use the dropdown menu to select the color that will be used as the background color when selecting text with the mouse. Sixteen colors are available for your selection. Teal is the default selection color.

Disconnected

Use the dropdown menu to select the color that will be used as the foreground color in a terminal window that has no connection to a remote host computer. Sixteen colors are available for your selection. Gray is the default foreground color for a disconnected terminal window.

Cursor Color

Select the desired cursor color from the dropdown menu. Sixteen colors are available for your selection. Blue is the default cursor color.

ANSI Colors

With ANSI control codes it is possible to change the color of text in a terminal window. With the ANSI Colors setting you can select if you want to allow this feature or not. Even if you disable ANSI colors, you

can still select your favorite text and background colors to be used in the terminal window.

Enable ANSI Colors

Check the Enable ANSI Colors check box to allow ANSI colors to be used in the terminal window.

Reverse Colors

By reversing the display colors you can quickly change the display from positive (dark on light) to negative (light on dark) to improve visibility.

Reverse Video

Check the Reverse Video check box to change the foreground color into background color and vice versa. This setting affects the whole terminal window as soon as you click the OK button.

2.4.5 Keyboard

The keyboard settings used for the connection are configured using the Keyboard page of the Settings dialog. Keyboard mappings take effect immediately when you close the Settings dialog, without needing to restart the connection.

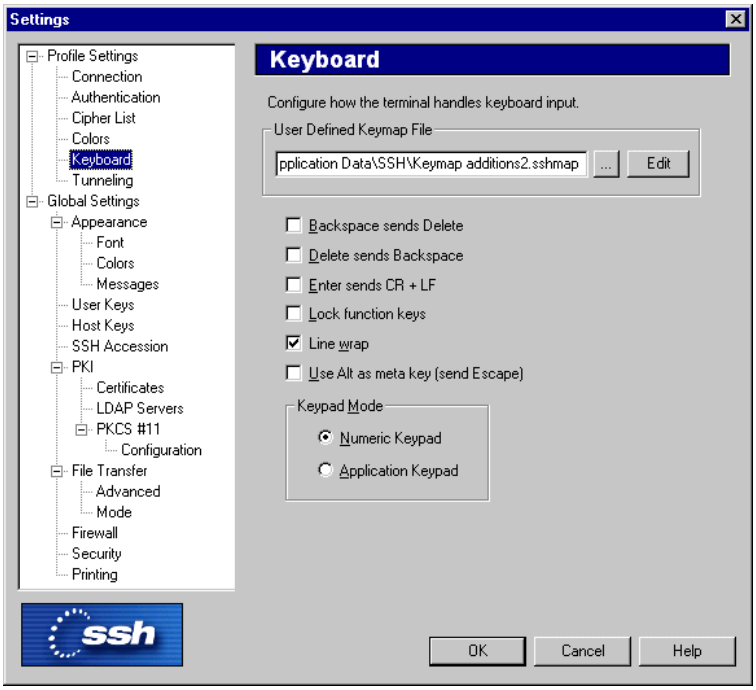

Figure 2.6: The Keyboard page of the Settings dialog.

User Defined Keymap File

With the User Defined Keymap File option you can create additional keyboard shortcuts or modify the existing ones. The additional key mappings are saved into a separate file with the `.sshmap` file extension. The current keymap file is displayed on the text field.

You can customize the current key mappings by clicking the **Edit** button. The Keymap Editor dialog will appear. For more information on using the Keymap Editor, see section 2.4.6 (Keymap Editor).

If you have an alternative keymap settings file already defined, you can load it by typing the path and file name in the text field, or by clicking on the button on the righthand side of the text field. Clicking the button will open an Open dialog that allows you to locate an alternative keymap file.

Backspace sends Delete

Select the **Backspace sends Delete** check box if you want to map the Backspace key to the Delete operation.

Delete Sends Backspace

Select the **Delete Sends Backspace** check box if you want to map the Delete key to the Backspace operation.

Enter sends CR + LF

Select the **Enter sends CR + LF** check box if you want to map the Enter key to send the carriage return (CR) and line feed (LF) characters. Otherwise only the line feed character will be sent.

Lock Function Keys

Select the **Lock Function Keys** check box if you want to lock the function keys.

Line Wrap

Select the **Line Wrap** check box if you want the text lines to wrap on the terminal window's edge. By default, line wrapping is on.

Use Alt as meta key (send Escape)

Select the **Use Alt as meta key (send Escape)** check box if you want the `Alt` key to function as the meta key in the same way as the `Escape` key. If this option is selected, you can for example press the `Alt+X` key combination to simulate the `Escape` followed by `X`.

Keypad Mode

Select how you want the numeric keypad on the right hand side of the regular keyboard to function.

Numeric Keypad: The keypad is used to type numbers.

Application Keypad: The keypad is used for application control (with the keypad keys functioning as cursor keys, Home, End, Page Up, Page Down, Insert and Delete).

2.4.6 Keymap Editor

The Keymap Editor dialog displays any customizations made to the current keymap. Using the editor you can define additional key mappings, open saved keymap files and create new keymap files.

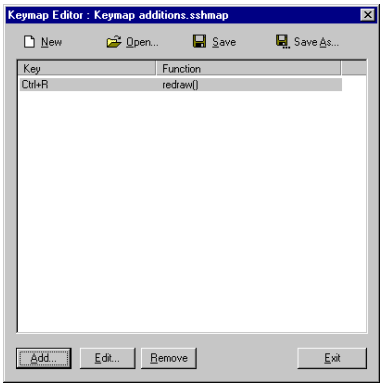

Figure 2.7: Customizing the keymap

The icons on the top of the Keymap Editor dialog allow you to open an already defined keymap file, to start a new keymap file from scratch, or to save the current keymap customizations into a keymap file:

New

Click the **New** button to start creating a new keymap file. This will clear all the current keymap customizations.

Open

Click the **Open** button to load an already defined keymap file for further customization. The Open dialog will appear, allowing you to locate the desired keymap file.

Save

Click the **Save** button to save the current keymap customizations to the currently open keymap file. If no keymap file has been loaded, the Save As dialog will open, allowing you to specify the file name for a new keymap file.

Save As

Click the **Save As** button to save the current keymap customizations into a different keymap file. The Save As dialog will open, allowing you to specify the file name for a new keymap file.

The large area in the center of the Keymap Editor dialog displays the defined keymap customizations. The **Key** column on the left displays the key combination whose function has been customized and the Function column displays the effect that pressing this particular key combination will cause.

The buttons on the bottom of the Keymap Editor dialog allow you to customize the keymap settings of the current keymap file:

Add

Click the **Add** button to add a new keymap customization. A small Keymap Editor dialog appears. Place the cursor on the Shortcut Key line and press a key combination on the keyboard to select which key binding you want to modify. The select the desired function for that keypress from the Function drop-down menu.

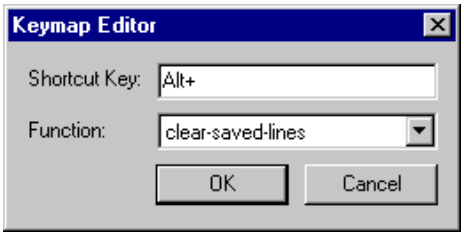

Figure 2.8: Modifying a keymap customization

Edit

Select an already defined keymap customization and click the **Edit** button to modify the selected customization.

Remove

Select an already defined keymap customization and click the **Remove** button to delete the selected customization.

Exit

Click the **Exit** button to close the Keymap Editor dialog. If you have not saved all your keymap customizations, a Confirm dialog will open, asking if you want to save the changes you have made or cancel the exit operation.

2.4.7 Tunneling

Tunneling settings are configured using the Tunneling page of the Settings dialog. Any changed tunneling settings will take effect the next time you login.

The outgoing and incoming tunnel settings are configured using the Outgoing and Incoming tabs of the Tunneling page.

Outgoing Tunnel

Outgoing tunnels protect data that your local computer sends from a specified local port to the specified port on the remote host computer. Click the **Outgoing** tab to edit outgoing tunnel definitions.

The following fields are used to define an outgoing tunnel. These values can be edited by clicking the Add or Edit buttons on the Outgoing page of the Settings dialog.

Display Name

The name of the tunnel definition. You can use this field to type in a descriptive name that will help you to recognize this tunnel definition later on.

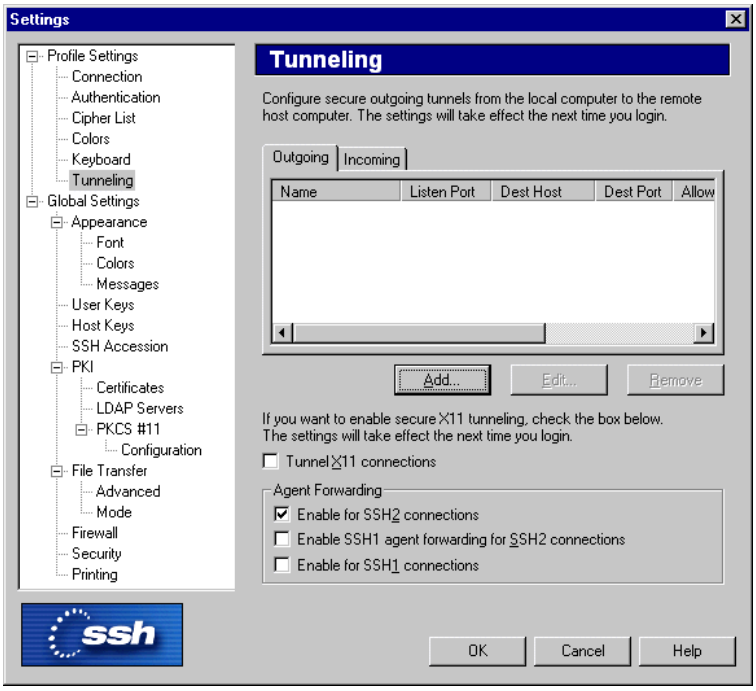

Figure 2.9: The Tunneling page of the Settings dialog.

Type

Select the type of the tunnel from the dropdown list. Valid choices are TCP and FTP.

Listen Port

This is the number of the port that the tunnel 'listens to', or captures.

Allow Local Connections Only

Leave a check mark in this box if you allow only local connections to be made. This means that other computers will not be able to use the tunnel created by you. By default, only local connections are allowed. This is the right choice for most situations. You should carefully consider the security implications if you decide to also allow outside connections.

Destination Host

This field defines the destination host of the tunnel. The default value is `localhost`.

Note: The value of `localhost` is resolved after the Secure Shell connection has been established - so `localhost` will refer to the remote host computer you have connected to.

Destination Port

The destination port defines what port will be used in the destination end of the tunnel.

Incoming Tunnel

Incoming tunnels protect the data that your local computer is receiving on a specified port from the remote host computer's specified port. Click the **Incoming** tab to edit incoming tunnel definitions.

The following fields are used to define an incoming tunnel. These values can be edited by clicking the Add or Edit buttons.

Display Name

The name of the tunnel definition. You can use this field to type in a descriptive name that will help you to recognize this tunnel definition later on.

Type

Select the type of the tunnel from the dropdown list. Valid choices are TCP and FTP.

Listen Port

The port that the tunnel 'listens to', or captures from the remote host computer.

Destination Host

This field defines the destination host of the tunnel. The default value is `localhost`.

Destination Port

The destination port defines what port will be used in the destination end of the tunnel.

Configuring Tunnels

The following buttons are available for configuring outgoing and incoming tunnels.

Add

Click the Add button to add a tunnel definition. An Add New Tunnel dialog appears, allowing you to define the name, type, listen port, destination host, and destination port of the tunnel. With outgoing tunnels you can also define if you allow local connections only.

Note that if you are tunneling an FTP connection, you must set the tunnel type as FTP.

Edit

Select a tunnel definition from the displayed list and click the Edit button to edit a previously defined tunnel. An Edit Tunnel dialog appears, allowing you to edit the name, listen port, destination host, and destination port of the outgoing tunnel. With outgoing tunnels you can also define if you allow local connections only.

Remove

Select a tunnel definition from the displayed list and click the Remove button to remove a previously defined tunnel. Note that the selected tunnel will be removed immediately, with no confirmation dialog being displayed.

Tunnel X11 connections

The Secure Shell 2 client can securely tunnel X11 connections from the remote host computer to an X-Windows server running on the local computer. Check the Tunnel X11 connections check box to enable secure X11 tunneling.

Note: You must also be running an X emulator such as *Exceed* or *Reflections X* on the Windows computer for X11 tunneling to work.

Agent Forwarding

Authentication agent (`ssh-agent2`) is a program to automatize the use of authentication private keys. When you use the agent, it will be automatically used for public-key authentication. This way, you only have to type the passphrase of your private key once to the agent. Furthermore, authentication data does not have to be stored on any other machine than the local machine, and authentication passphrases or private keys never go over the network.

Agent forwarding can be enabled or disabled based on the ssh protocol used. Select the check box for any of the options you want to use:

Enable for SSH2 connections

Agent forwarding can be used for SSH2 connections.

Enable SSH1 agent forwarding for SSH2 connections

SSH1 agent forwarding can be used for SSH2 connections.

Enable for SSH1 connections

Agent forwarding can be used for SSH1 connections.

2.5 Global Settings

Global configuration settings are configured using the Global Settings page of the Settings dialog. Global settings are common for all remote host computers.

Global settings are saved at the same time as profile settings. Global settings are always saved in the user profile directory with the filename `global.dat`.

2.5.1 Appearance

The appearance of the application and the terminal window is configured using the Appearance page of the Settings dialog.

Figure 2.10: The Global Settings page of the Settings dialog.

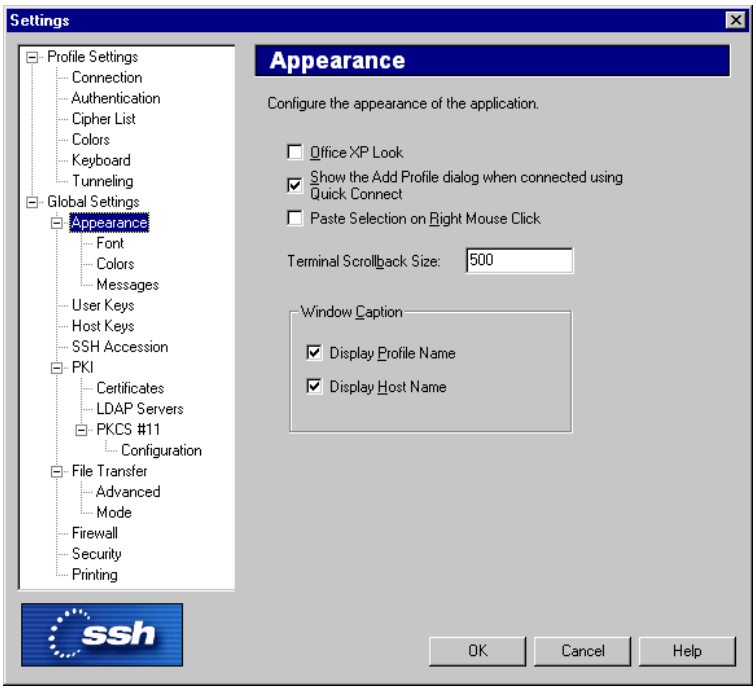

Figure 2.11: The Appearance page of the Settings dialog.

Office XP Look

Select the **Office XP Look** check box to change the way the menu bar and tool bar are displayed to

match the visual style of Microsoft Office XP.

Show Add Profile Dialog when connected using Quick Connect

Select the **Show Add Profile Dialog when connected using Quick Connect** check box to briefly display the Add Profile dialog when connecting to a remote host computer using Quick Connect. This allows you to create a profile for the host simply by typing in the profile name.

Paste Selection on Right Mouse Click

Select the **Paste Selection on Right Mouse Click** check box to enable fast copying of text on the terminal display. When you have this option selected, you can copy text simply by highlighting it and then paste it by clicking the right mouse button.

Terminal Scrollback Size

Type in the **Terminal Scrollback Size** field the number of lines that you want to collect in the scrollback buffer. The larger the value, the more you can scroll back the terminal display to view previous terminal output. The default value is 500 lines.

Window Caption

The **Window Caption** settings affect what is displayed in the title bar of the SSH Secure Shell for Workstations Windows client terminal window and the File Transfer window.

Display Profile Name

Select the **Display Profile Name** check box to have the name of the current profile to be displayed on the title bar.

Display Host Name

Select the **Display Host Name** check box to have the host name of the currently connected remote host computer to be displayed on the title bar.

2.5.2 Font

The font used in the terminal window can be selected using the Font page of the Settings dialog. The new font setting affects the terminal window immediately when you click the OK button. To discard the changes, click the Cancel button.

Font Name

Select the desired font from the Font Name list. The list displays the non-proportional (fixed-width) fonts installed in your local computer. Note that proportional fonts are not suitable for the terminal window and therefore are not available for selection.

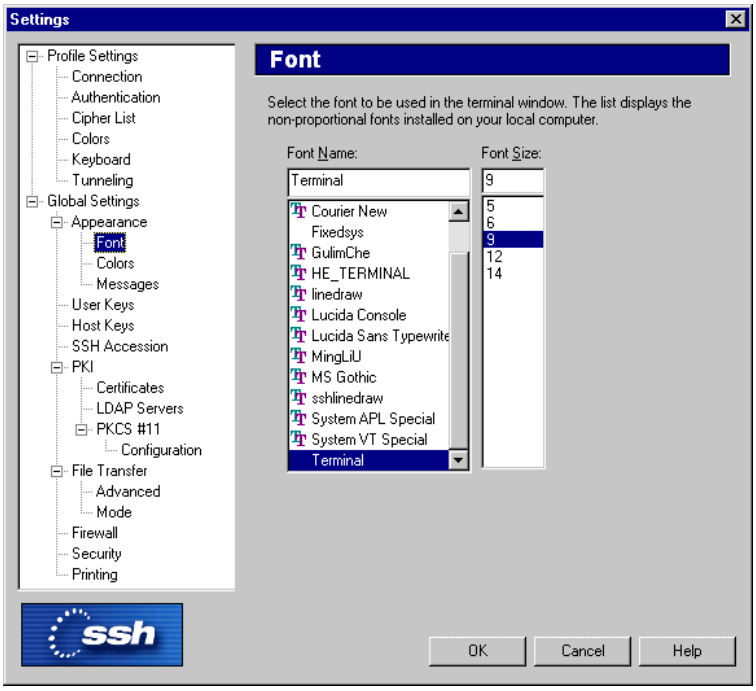

Figure 2.12: The Font page of the Settings dialog.

Font Size

Select the desired font size from the Font Size list. Note that the font size affects the size of the terminal window: the smaller font you select, the smaller the terminal window will be, and vice versa. However, after this operation the size of the terminal window can be modified to suit your tastes.

2.5.3 Colors

The color settings can be defined either globally or per profile. When the colors are defined under the Global Settings display, the Use Global Colors option is not available, but the color settings will affect all connection profiles.

For more information, see section 2.4.4 (Colors).

2.5.4 Messages

On the Messages page of the Settings dialog you can configure default replies to system messages that normally ask for user confirmation.

The messages are listed under several categories. Categories that have a plus sign (+) next to them can be expanded by clicking on the plus sign. Expanded categories have a minus sign (-) next to them and can be closed by clicking on the minus sign.

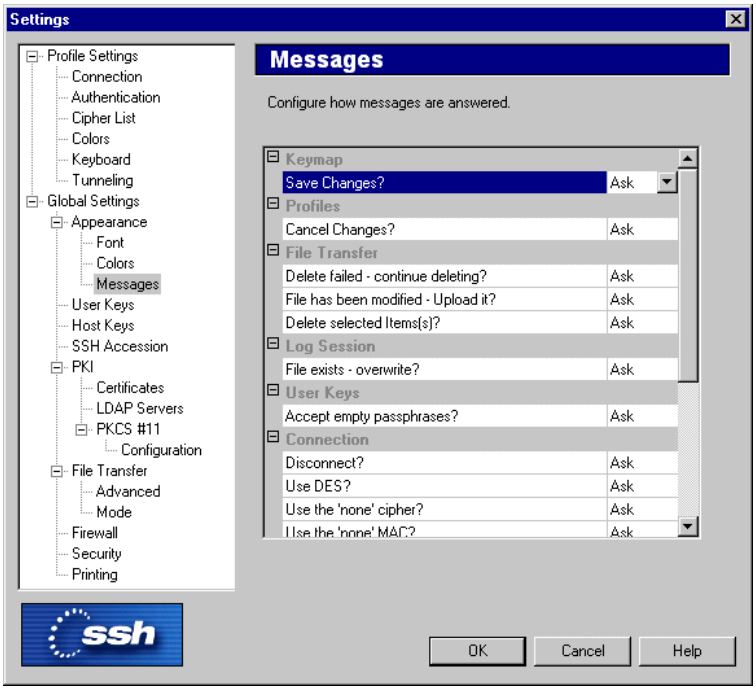

Figure 2.13: Customizing which confirmation dialogs are displayed

Each confirmation can be set to automatically accept (`Yes`) or reject (`No`) the action, or to ask the user for confirmation (`Ask`). By default all messages ask the user to confirm the action.

2.5.5 User Keys

Key pairs used for user public-key authentication can be managed using the User Keys page of the Settings dialog.

Note that your private keys should always be kept secret. This is important to remember if you are sharing your local computer with other users. In such case, it is not advisable to store your private keys in the local disk. For more information on user key files, see section 3.6 (Using Public-Key Authentication).

Generate New Keypair

Click the Generate New Keypair button to create a new public and private user key pair. This will bring up the Key Generation Wizard. For more information on this procedure, see section 3.3.1 (Key Generation Wizard).)

Delete Keypair

Select a key file from the private key file list and click the Delete button to delete the key file from your local computer.

Export Keypair

Figure 2.14: The User Keys page of the Settings dialog.

Select a key file from the private key file list and click the Export Keypair button to export the key pair. A Select Folder dialog will open, allowing you to specify the target location.

Import Keypair

Click the Import Keypair button to import a keypair. The Import Keypair - Select Files dialog will open, allowing you to locate the keypair to be imported.

View Public Key

Select a previously generated private key file from the private key file list and click the View Public Key button to display the corresponding public key. The public key file will be displayed in Notepad.

Change Passphrase

Select a previously generated private key file from the private key file list and click the Change Passphrase button to change the passphrase for the key.

Upload Public Key

Clicking the Upload Public Key button while connected to a remote server will automatically upload the selected public key. For more information on this procedure, see section 3.5 (Uploading Your Public Key).

Private key file list

The private key file list (located above the buttons on the User Keys page) shows the files used to store your private keys. The public keys are not displayed, as they have the same file names as the private keys, but with

`.pub` as the file extension.

Private Key File Name

The Private Key File Name column displays the file names of your private keys.

Comment

The Comment column displays the comments (if any) associated with your private keys.

2.5.6 Host Keys

Public host keys used in remote host authentication process can be managed using the Host Keys page of the Settings dialog. The keys are listed in the host key file list.

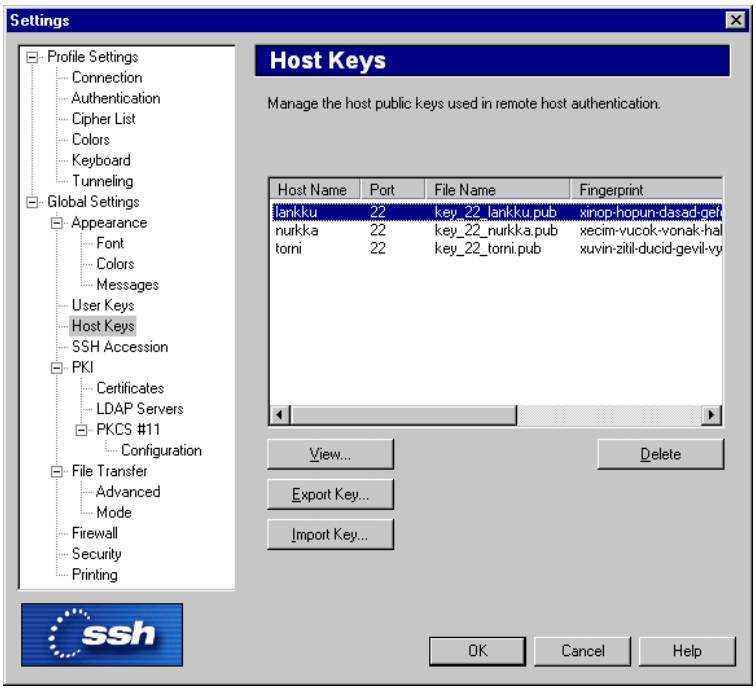

Figure 2.15: The Host Keys page of the Settings dialog.

View

Select a host key file from the host key file list and click the View button to display a host key. Alternatively you can just double-click on the key file name.

Export Key

Select a host key and click the Export Key button to export a host key. The Select Folder dialog will open, allowing you to specify the target location.

Import Key

Click the Import Key button to import a host key. The Import Hostkeys - Select Files dialog will open, allowing you to locate the host key to be imported.

Delete

Select a host key file from the host key file list and click the Delete button to delete the key.

Host key file list

The host keys in your possession are displayed in the host key file list (located above the buttons on the Host Keys page).

Host Name

The Host Name column displays the host names of your host keys.

Port

The Port column displays the ports used by the connections associated with each host key.

File Name

The File Name column displays the file name of each host key file.

Fingerprint

The Fingerprint column displays the fingerprint of each host key file. The fingerprint is represented using the SSH Babble format, and it consists of a pronounceable sets of five lowercase letters separated by dashes.

2.5.7 SSH Accession

On the SSH Accession page of the Settings dialog you can operate the keys and certificates that are available on SSH Accession. SSH Accession is a separate software product by SSH Communications Security that offers an easy method for utilizing digital certificates and smart cards.

Upload Public Key

Select a public key from the list and click the **Upload Public Key** button to upload the key.

View Certificate

Select a certificate from the list and click the **View Certificate** button to display the contents of the certificate.

Figure 2.16:

2.5.8 PKI

Public Key Infrastructure (PKI) is a system where digital certificates are used to increase the reliability and scalability of authentication. Using certificate authentication requires that certificates are first created with certification authority (CA) software.

The PKI page displays a short introduction to the concept of PKI.

For more information about public-key infrastructure, see section 8.2 (Public Key Infrastructure (PKI)).

Please note that PKI and PKCS #11 support is only available in commercial distributions of the SSH Secure Shell for Workstations client.

2.5.9 Certificates

The Certificates page (visible only in commercial distributions) of the Settings dialog can be used to control certificates created by a certification authority (CA) software.

Certificate list

The available certificates are shown in the certificate list, located on the top of the Certificates page. This list can be used to view both personal certificates and trusted certification authorities.

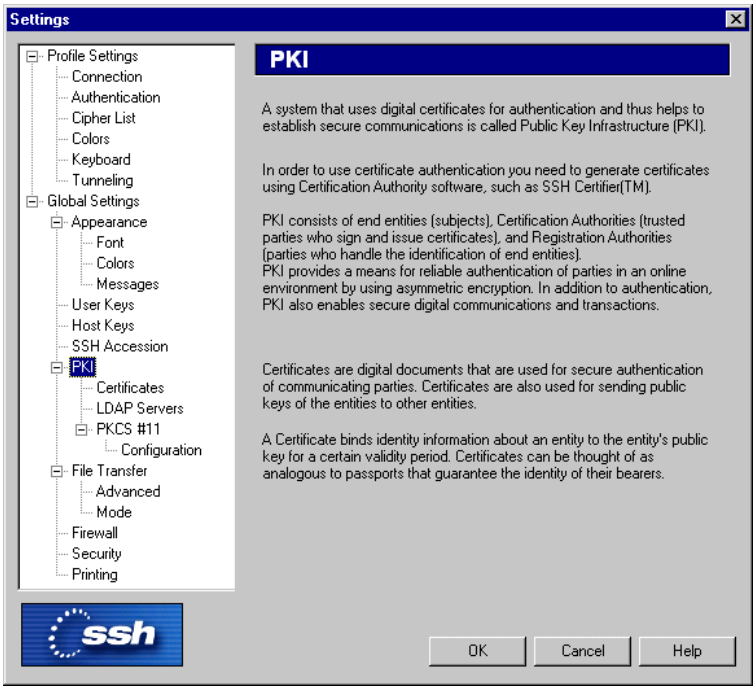

Figure 2.17: A brief overview of PKI.

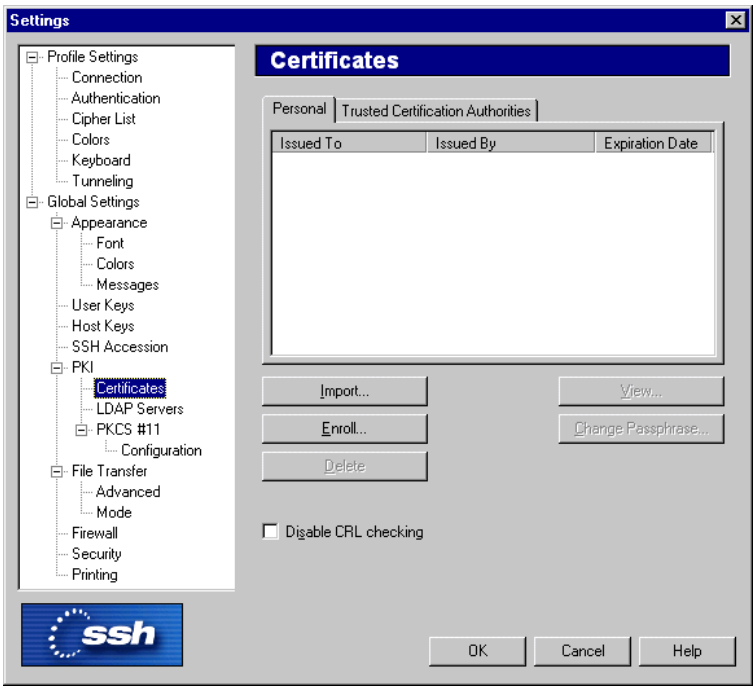

Figure 2.18: The Certificates page.

Personal

Click the Personal tab to display your personal certificates.

Trusted Certification Authorities

Click the Trusted Certification Authorities tab to display the trusted Certification Authorities.

The following fields are displayed on the certificate list:

Issued To

The Issued To field shows the entity to whom the certificate has been issued.

Issued By

The Issued By field shows the entity who has issued the certificate.

Expiration Date

The Expiration Date field shows when the certificate will expire.

The following buttons can be used to control the certificates:

Import

Click the Import button to import a certificate created with certification authority (CA) software. A file selection dialog will open, allowing you to browse your directories for the saved certificate file.

Enroll

Click the Enroll button to start the Certificate Enrollment wizard, which is used to request a certification authority (CA) to issue a certificate. SSH Secure Shell supports the CMPv2 enrollment protocol.

For more information on the process, see section 2.5.10 (Certificate Enrollment Wizard).

Delete

Click the Delete button to remove a selected certificate.

View

Click the View button to display the contents of a selected certificate.

Change Passphrase

Click the Change Passphrase button to type a new passphrase associated with the selected certificate.

Disable CRL Checking

Select the Disable CRL Checking check box to prevent the use of a certificate revocation list (CRL). A CRL is used to check if any of the used certificates have been revoked.

2.5.10 Certificate Enrollment Wizard

The Certificate Enrollment wizard (available only in commercial distributions) is used to enroll certificates, i.e. to request a certification authority (CA) to issue a certificate. You can start the wizard by clicking on the Enroll button of the Certificates page of the Settings dialog.

Certificate Enrollment - Start

The first page of the Certificate Enrollment wizard displays information on the enrollment process. The enrollment process will create both a public and a private key. Please note that the process requires the use of Certificate Management Protocol version 2 (CMPv2).

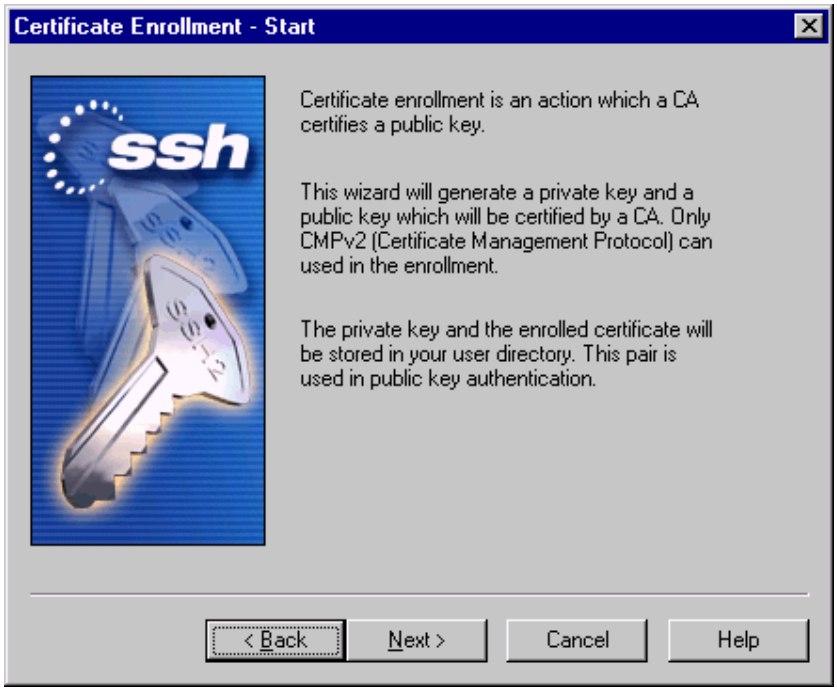

Figure 2.19: The start of the enrollment process.

Click the Next button to continue the process.

Certificate Enrollment - Identity

On the **Identity** page, enter the parameters of the certificate to be issued. You can suggest a Common Name (e.g. *John Smith*), Organization Unit (like *Marketing*), Organization (*SSH Communications Security Corp.*), Country (*US*) and Email Address (*john.smith@ssh.com*).

The certification authority can change these fields before issuing the certificate. The Certificate validity period and other parameters are determined by the configuration of the CA software.

Please note that certificate enrollment requiring manual acceptance in the CA software is not supported. You may be able to compensate for this by using PKCS #12 file importing.

Click the Next button to launch the Key Generation Wizard. For more information on the key generation process, see section 3.3.1 (Key Generation Wizard).

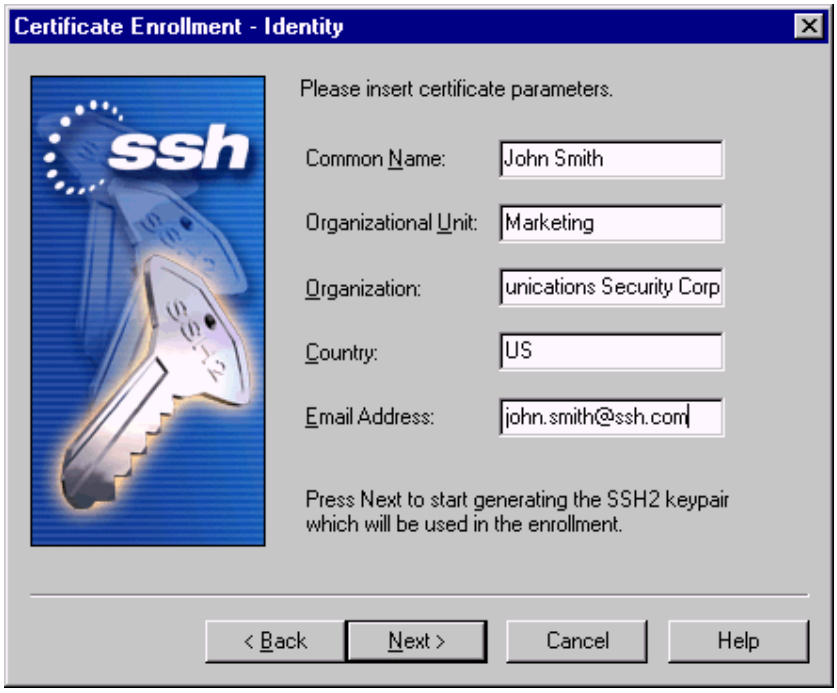

Figure 2.20: Type the parameters of the certificate.

Certificate Enrollment - Firewall

On the **Firewall** page, you can define the firewall and proxy settings. These fields can be left empty.

Firewall

Type the firewall location in the text field.

HTTP proxy

Type the HTTP proxy location in the text field.

Click the **Next** button to continue.

Certificate Enrollment - CA

On the **CA** page, fill in the following fields:

CA URL

Type in the certification authority (CA) address.

Discover

Click the **Discover** button to attempt automatic detection of available certification authority services and CA certificates. The found CA services will be listed in the text field and can be selected from the drop-down menu.

Please note that not all systems support the automatic detection functionality.

CA Certificate

Type in the file name of the certificate, or select the file by clicking on the button on the right hand side of the file name field. The **Select CA Certificate** dialog will open, allowing you to locate the certificate file.

View

Click the **View** button to display the contents of the current certificate.

Retrieve CA Certificates from CA URL

Select the desired CA URL from the drop-down list and click the **Retrieve CA Certificates from CA URL** button to retrieve the CA certificates from the selected CA address.

Reference Number

Type in the reference number.

Key

Type in the key information.

Click the **Next** button to continue.

Certificate Enrollment - Enrollment

On the Enrollment page the actual enrollment takes place. This may take some time (the exact duration depends on the amount of network traffic, among other factors).

When the process is finished, click the Finish button to continue.

2.5.11 LDAP Servers

In order to make use of the certificate, it must be distributed to directories, where it is available to other PKI users. SSH Secure Shell supports certificate and certificate revocation lists (CRL) distribution using Lightweight Directory Access Protocol (LDAP).

(Please note that PKI and PKCS #11 support is only available in commercial distributions of the SSH Secure Shell for Workstations client.)

The LDAP Servers list displays the available LDAP servers.

Figure 2.21: The enrollment in progress.

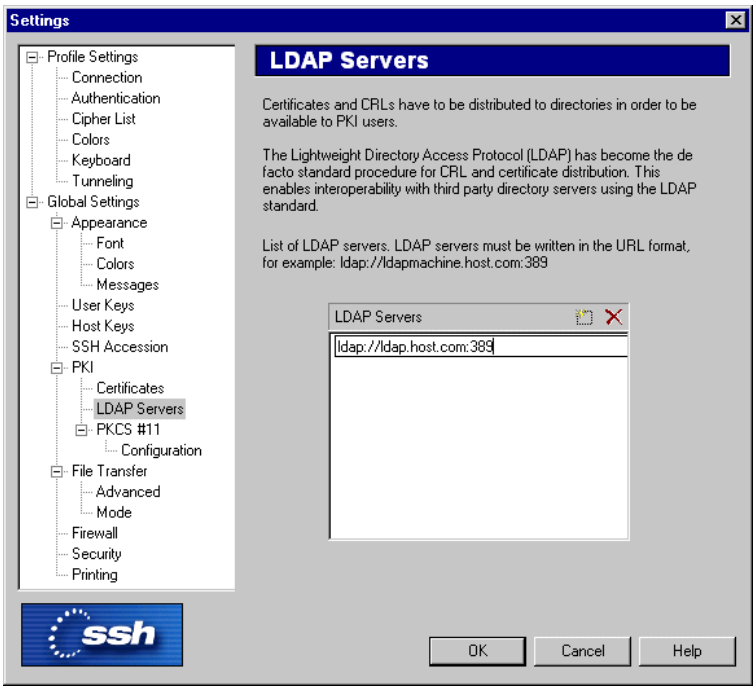

Figure 2.22: Adding a new LDAP server entry.

New

Click the New button (the leftmost button on the top right hand side of the LDAP server list) to add

a new LDAP server to the list. Type in the address of the server using URL format. The keyboard shortcut for the New button is the `Ins` key.

Delete

Select an unwanted LDAP server entry from the list and then click the Delete button (the rightmost button on the top right hand side of the LDAP server list) to remove the server definition. The keyboard shortcut for the Delete button is the `Delete` key.

2.5.12 PKCS #11

The PKCS #11 page (visible only in commercial distributions) contains a list showing the configured PKCS #11 providers. Under each provider is a list of the keys and certificates available. Please note that the list view does not update automatically, but only when you close and reopen it.

A new provider can be added to the list on the Configuration page of the Settings dialog. For more information, see section 2.5.13 (Configuration).

Figure 2.23: The PKCS #11 providers list.

You can open the PKCS #11 configuration window by double-clicking the card reader icon located on the right hand side of the SSH Secure Shell terminal window status bar, located on the bottom of the window.

Hardware tokens and PKCS #11 software keys can be used with or without PKI. The standard public-key authentication can be used with PKCS #11 providers.

The following buttons can be used to operate the PKCS # providers:

Enable Provider

Select a PKCS #11 provider from the list and click the Enable Provider button to allow the use of the selected provider.

Disable Provider

Select a PKCS #11 provider from the list and click the Disable Provider button to disallow the use of the selected provider.

Upload Public Key

Select a key from the list and click the Upload Public Key button to upload one of the public keys from the token to the server. This allows you to use a hardware token for your personal authentication. In order to do this, you have to be already connected to a server.

Please note that an RSA token requires RSA support to be compiled in the server software. See section 3.5 (Uploading Your Public Key) for information on how to upload a software public key to the server.

View Certificate

Click the View Certificate button to display the contents of the selected certificate.

2.5.13 Configuration

The Configuration page of the Settings dialog can be used to manually configure PKCS #11 providers.

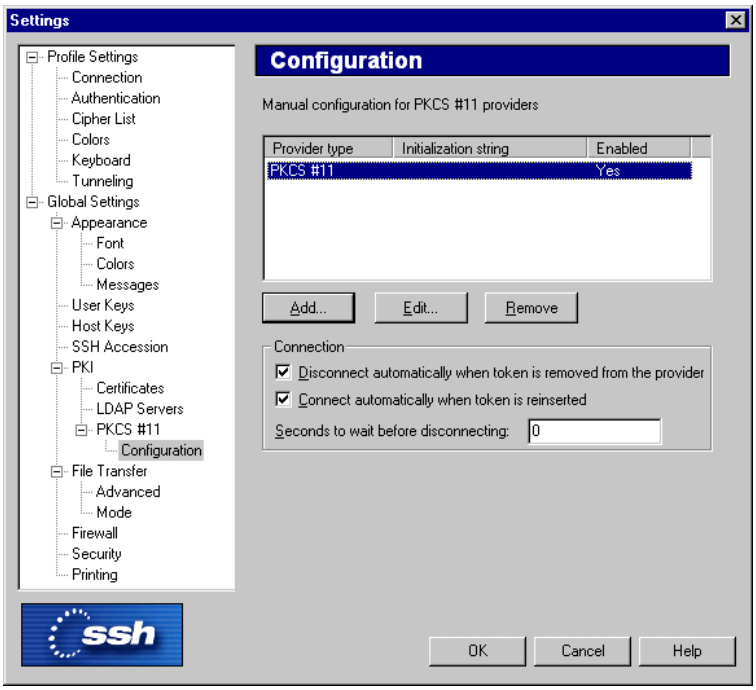

Figure 2.24: Configuring PKCS #11 providers.

The following fields are visible in the provider list, displayed on the top of the Configuration page:

Provider Type

The Provider Type field displays the type of the provider.

Initialization String

The Initialization String field displays the string of characters used for initialization.

Enabled

The Enabled field displays whether the use of the provider is currently allowed or not. To change the Enabled status, click the Edit button.

The following buttons can be used to control the provider settings:

Add

Click the Add button to add a new PKCS #11 provider. The PKCS #11 Provider dialog will open.

Edit

Click the Edit button to change the details of the PKCS #11 provider. The PKCS #11 Provider dialog will open.

Remove

Click the Remove button to delete the PKCS #11 provider definition.

For more information on the PKCS #11 Provider dialog, see section 2.5.14 (PKCS 11 Provider).

Connection

Also the following connection settings can be specified on the Configuration page:

Disconnect automatically when token is removed from the provider

Select this check box to ensure that a connection will be active only when a token is present.

Connect automatically when token is reinserted

Select this check box to allow automatical connection to be established when the token is again inserted.

Seconds to wait before disconnecting

Type in the text field the number of seconds to wait before the connection is lost when a token is removed. This field is active only if the *Disconnect automatically when token is removed from the provider* check box is selected.

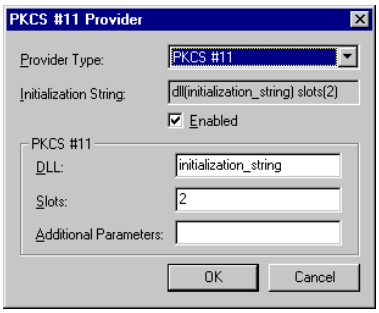

Figure 2.25: The details of the PKCS #11 provider displayed.

2.5.14 PKCS #11 Provider

The PKCS #11 Provider dialog allows you to view and modify the provider definition.

The following options are available:

Provider Type

Select the provider type from the dropdown menu.

Initialization String

This field displays the character string used for initialization.

Enabled

Leave the Enabled check box checked, except if you have trouble accessing the token from another application that is running simultaneously. The usability of a PKCS #11 for several simultaneous applications depends on the specific third party PKCS #11 driver.

PKCS #11

Fill in the following text fields to pass other parameters to the PKCS #11 provider:

DLL

Consult the token manufacturer documentation to determine the file name of the PKCS #11 DLL. Type this file name in the DLL field.

Slots

The Slots parameter is not required, but if you have problems accessing a specific key on a hardware token, you may need to modify this parameter accordingly. Consult the third party documentation for the exact requirements of the Slots parameter.

For example: to use PKCS #11 slots 0 through 10, use the value `0-10`, and to use slots 1 through 5 except 3, use the value `1-5,!3`.

Additional Parameters

Additional parameters can be specified, if specified in the third party documentation.

When you save the settings (by using the Save Settings option on the File menu) and then restart SSH Secure Shell, you should see a small card reader icon on the status bar on the bottom of the terminal window. When a token is inserted, a smart card appears in the card reader in the icon. When a key is acquired from the token, a key symbol appears on top of the card reader icon.

If you do not see the card reader icon, check that the DLL name has been entered correctly. If you cannot get the keys from the token, make sure that the token has been personalized correctly. Please note that hardware tokens are usually shipped uninitialized, so you are required to personalize the token for yourself. To do this, you need to consult the third party documentation included with the token.

2.5.15 File Transfer

The default file transfer settings can be configured using the File Transfer page of the Settings dialog. The new settings will affect subsequently started File Transfer windows.

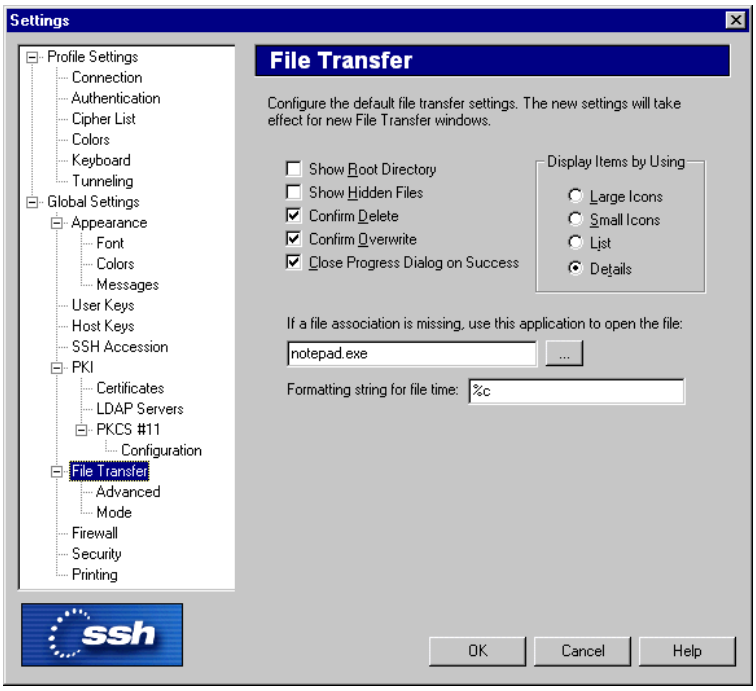

Figure 2.26: The File Transfer page of the Settings dialog.

Show Root Directory

Check the Show Root Directory check box to show the root directory in the File Transfer window by default.

Show Hidden Files

Check the Show Hidden Files check box to show hidden files in the File Transfer window by default.

Confirm Delete

Check the Confirm Delete check box if you want the File Transfer utility to ask for confirmation when deleting files or folders.

Confirm Overwrite

Check the Confirm Overwrite check box if you want the File Transfer utility to ask for confirmation when you try to transfer a file that already exists in the target system.

Close Progress Dialog On Success

Check the Close Progress Dialog On Success check box if you want that the Download and Upload dialogs close automatically when finished.

Display Items by Using

With the Display Items by Using setting you can select the default view for the File Transfer window by choosing one of the four possible views.

Large Icons

Select the Large Icons option to display the File Transfer file view as a Large Icons view. Each file and folder has a large icon associated with it, making for a clear and uncluttered display.

Small Icons

Select the Small Icons option to display the File Transfer file view as a Small Icons view. Each file and folder has a small icon associated with it. This makes it possible to display several times more items than the Large Icons view.

List

Select the List option to display the File Transfer file view as a List view. Each file and folder has a small icon associated with it, and the files and folders are displayed in one single column underneath each other.

Details

Select the Details option to display the File Transfer file view as a Details view. The files and folders are displayed with a small icon, their file name, file size, file type, their last modification date and attributes visible.

By clicking on the Name, Size, Type and Modified sort bars located on top of the File view, you can sort the files and folders based on their file name, file size, file type and the time they were last modified. Clicking the same sort option again reverses the sorting order.

Note that the sort function is not case sensitive: upper case text is sorted together with lower case text.

The file type associations are derived from the your local computer. If you have defined a new file type description for files with a certain file name extension, also the files in the remote computer are shown to be of that file type. This makes it easy to recognize particular file types also on the host computer.

Missing File Association

The SSH Secure Shell for Workstations Windows client uses file type associations in the same way as Windows Explorer does. When you double-click a file in the File Transfer window, it will be opened using the application with which its file type has been associated.

All file types are not associated with any application. With this field you can define what application will be used to open a file that has no file type association. The default application is Notepad, which is a reasonable choice for files containing text.

To change the default association for unknown file types, click the button next to the text field. A Select Application dialog will be displayed, allowing you to select the desired application.

Formatting string for file time

In the formatting string field you can type a string that presents how the time and date stamps of the files are displayed in the File Transfer window. The default value is `%c`, which means that the date and time will be presented in the format defined in the Windows country settings (locale).

To change the format of the time and date stamps, replace the default value with a string consisting of some of the following character combinations.

%a

Abbreviated weekday name

%A

Full weekday name

%b

Abbreviated month name

%B

Full month name

%c

Date and time representation appropriate for locale

%d

Day of month as decimal number (01 - 31)

%H

Hour in 24-hour format (00 - 23)

%I

Hour in 12-hour format (01 - 12)

%j

Day of year as decimal number (001 - 366)

%m

Month as decimal number (01 - 12)

%M

Minute as decimal number (00 - 59)

%p

Current locale's A.M. / P.M. indicator for 12-hour clock

%S

Second as decimal number (00 - 59)

%U

Week of year as decimal number, with Sunday as first day of week (00 - 53)

%w

Weekday as decimal number (0 - 6; Sunday is 0)

%W

Week of year as decimal number, with Monday as first day of week (00 - 53)

%x

Date representation for current locale

%X

Time representation for current locale

%y

Year without century, as decimal number (00 - 99)

%Y

Year with century, as decimal number

%z, %Z

Time-zone name or abbreviation; no characters if time zone is unknown

%%

Percent sign

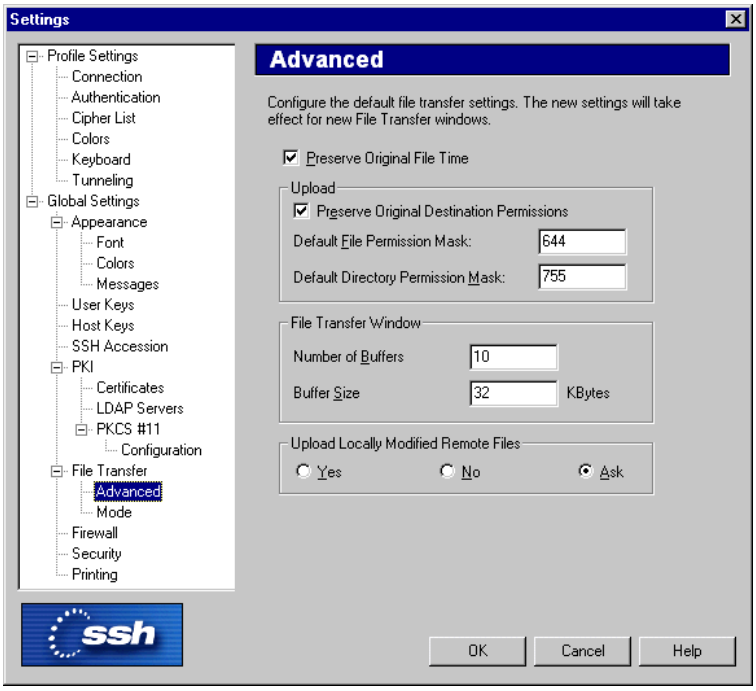

Figure 2.27: Even more file transfer options displayed.

2.5.16 Advanced

On the Advanced page of the Settings dialog you can configure additional file transfer options. The new settings will affect subsequently started File Transfer windows.

Preserve Original File Time

Check the Preserve Original File Time check box if you want that the transferred files retain their original time and date stamp values. If this option is not selected, the transferred files will be stamped with the time of the transfer.

Upload

The following settings affect the upload process

Preserve original destination permissions

Select this check box to preserve the file permissions of the original file located on the remote host computer. The transferred file will use the same file permissions as the original file.

Default file permission mask

Type the octal UNIX file permission mask (as with the `chmod` command) that is to be used as the default value for files.

Default directory permission mask

Type the octal UNIX directory permission mask (as with the `chmod` command) that is to be used as the default value for directories.

File Transfer Window

The following settings affect the file transfer process:

Number of buffers

Type the number of buffers used in file transfer. The default value is 10.

Buffer size

Type the default buffer size. The default value is 32 kilobytes.

Upload Locally Modified Remote Files

This selection affects how SSH Secure Shell will react if you edit locally a file stored in the remote host computer.

Yes

If you select the Yes option, the locally modified file will be uploaded to the remote host computer.

No

If you select the No option, the locally modified file will not be uploaded to the remote host computer.

Ask

If you select the Ask option, SSH Secure Shell will ask you to decide if you want to upload a locally modified file.

2.5.17 Mode

The Mode page of the Settings dialog affects which files will be transferred using ASCII mode.

File Transfer Mode

Select the default file transfer mode from the following options:

ASCII

By default all files will be transferred in ASCII mode.

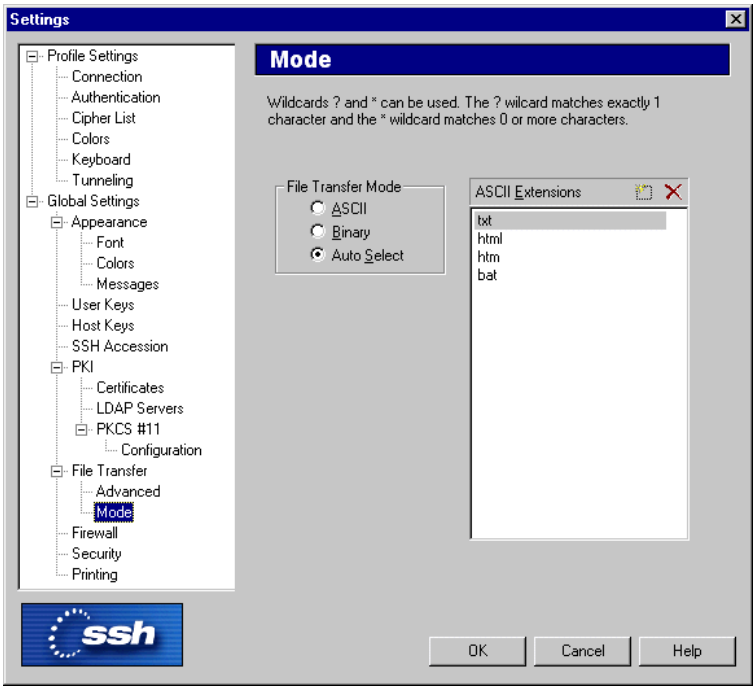

Figure 2.28: Selecting the file transfer mode.

Binary

By default all files will be transferred in binary mode.

Auto Select

The files using a file extension specified on the ASCII Extensions list will be transferred in ASCII mode. All other files will be transferred in binary mode.

ASCII Extensions

Files using a file extension specified in the ASCII Extensions list will be transferred using ASCII mode.

New

Click the New button (the leftmost button on the top right hand side of the ASCII Extensions list) to add a new file extension to the list. The keyboard shortcut for the New button is the `Ins` key.

Note that you can use wild cards to specify the file extensions. The `?` character matches any 1 character, and the `*` character matches any 0 or more characters.

Delete

Select an unwanted file extension entry from the list and then click the Delete button (the rightmost button on the top right hand side of the ASCII Extensions list) to remove the extension. The keyboard shortcut for the Delete button is the `Delete` key.

2.5.18 Firewall

The firewall settings can be configured using the Firewall page of the Settings dialog. The firewall should run SOCKS version 4 software.

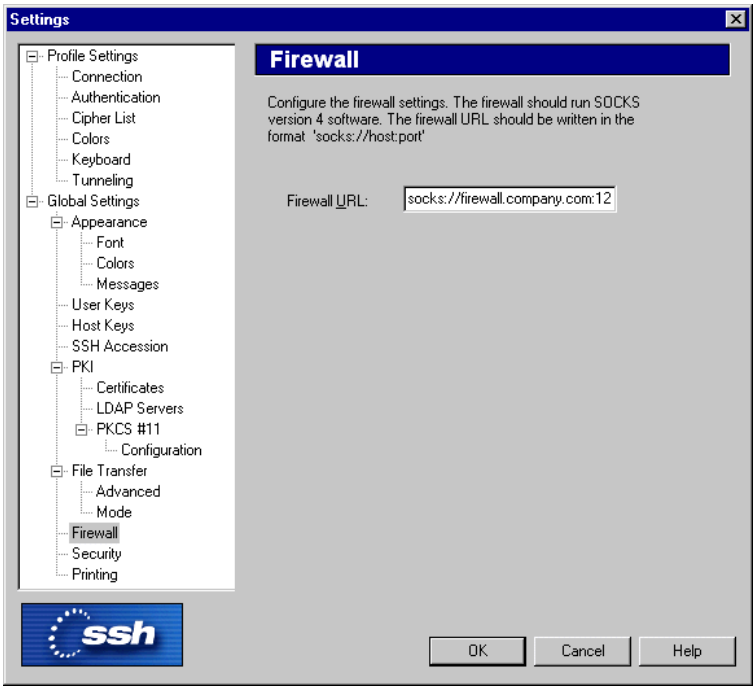

Figure 2.29: The Firewall page of the Settings dialog.

Firewall URL

Type the firewall address in URL format (for example `socks://host.computer:1080`).

2.5.19 Security

The security settings can be configured using the Security page of the Settings dialog.

Clear Host Name

Select the **Clear Host Name** check box to avoid displaying the previous remote host computer name in the login dialog.

Clear User Name

Select the **Clear User Name** check box to not display the previous user name in the login dialog.

Empty Clipboard on Exit

Select the **Empty Clipboard on Exit** check box to remove from the clipboard anything that was recently copied using the cut and paste Edit operations.

Figure 2.30: The Security page of the Settings dialog.

Empty Scrollback Buffer on Session Close

Select the **Empty Scrollback Buffer on Session Close** check box to empty any remains of the terminal output from the scrollback buffer.

SSH1 Connections

From SSH Secure Shell for Workstations Windows client version 2.2.1 onwards, you can connect also to SSH version 1 (ssh1) servers. With the ssh1 Connections selection you can decide if you want to allow ssh1 connections, deny them, or issue a warning when connecting to a remote host computer that is using version 1 of the SSH protocol.

SSH version 2 (ssh2) is a more advanced and secure protocol than the legacy version ssh1. For more information on using an ssh1 connection, see the SSH web site `http://www.ssh.com/products/ssh/ssh1.html`.

Note that when using an ssh1 connection, multiple terminal windows and the file transfer operations are not available.

Allow

Select this option to allow also ssh1 connections.

Warn

Select this option to issue a notice when an ssh1 connection is made.

Deny

Select this option to disallow ssh1 connections.

Disable password length masking in SSH1 connections

Select this check box to not use password length masking when logging in using the ssh1 protocol.

2.5.20 Printing

The print settings can be configured using the Printing page of the Settings dialog. (Print Settings can also be selected from the File menu of the terminal window.)

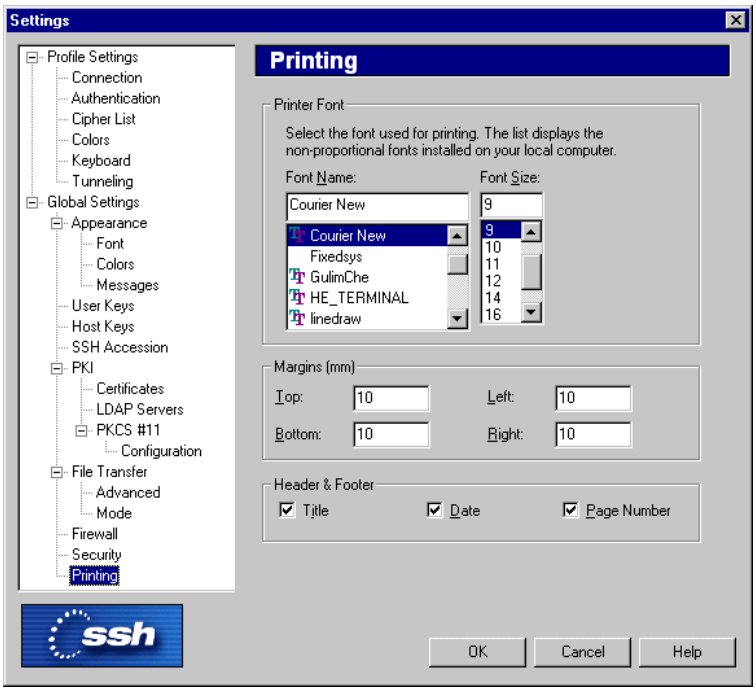

Figure 2.31: The Printing page of the Settings dialog.

Printer Font

Select the font and font size to be used in the printed output. Any non-proportional font installed on your system can be selected.

Margins

Select the width of the blank border around the page on printed output. The margins for the top, bottom, left and right of the page can all be specified individually. The default value for all margins is 10 millimeters.

Header & Footer

Select what additional information appears on the printed pages.

Title appears at the top left of the page and displays the title of the terminal window (for example: `remotehost - SSH Secure Shell`).

Date appears at the top right of the page and displays the date and time when the page was printed (for example: `07 December 2000, 05:47`). The date and time format is the same as used in Windows.

Page Number appears at the bottom right of the page (for example: `Page 1 of 2`).

2.6 Customize

Select the Customize option from the View menu to modify the menu options, toolbars layout, keyboard mapping, menu settings and general preferences. Note that you can have only one terminal window open when using the Customize option.

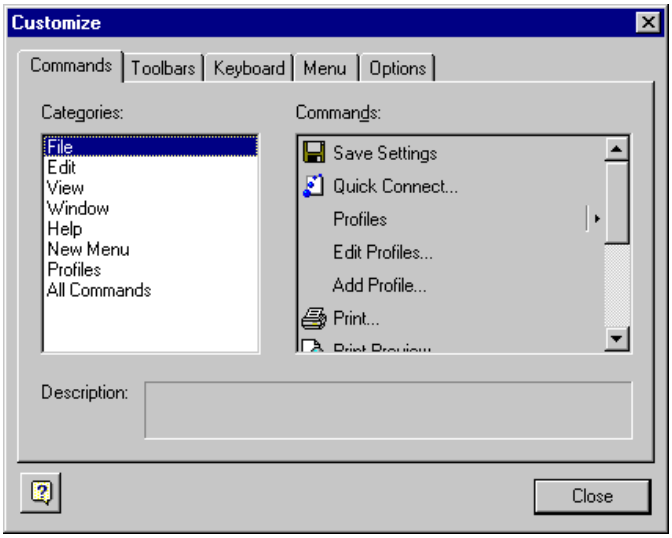

Figure 2.32: Use the Customize dialog to modify the user interface settings.

Click on the tabs on the top of the dialog to switch between different pages:

Commands tab

Select the Commands tab to move individual menu options. Select the menu category from the list on the left, and then use the mouse to drag menu options into the menus or toolbars displayed in the SSH Secure Shell window.

Toolbars tab

Select the Toolbars tab to define which toolbars are displayed on the SSH Secure Shell window.

If you have made any changes, you can select the toolbars you want reset and then click the Reset button to return the default toolbar configuration. Click the Reset All button to reset all the toolbars and menus.

Select either the Profiles or Toolbar option and then check the Show text labels check box to display text labels on these toolbars. Text labels clarify the toolbar icons, but also take up space.

Keyboard tab

Select the Keyboard tab to define accelerator keys (keyboard shortcuts) for the menu commands.

Use the Category menu to select the category of the accelerator key you want to modify. The categories are based on the menu hierarchy.

Use the Commands menu to select a specific command from the selected category.

The Description box displays a brief description of the currently selected command.

Use the Set Accelerator for menu to select the profile that you want to associate with the current keyboard configuration.

The Current Keys field shows the currently assigned accelerator keys.

Click on the Press New Shortcut Key field to activate it. Then press the combination of keys on the keyboard that you want to associate with the currently selected command.

Click the Assign button the add the definition from the Press New Shortcut Key field to the Current Keys field.

Select a key assignment from Current Keys field and click the Remove button to delete the selected assignment.

Click the Reset All button to lose all your changes and reset the keyboard assignments. A confirmation dialog will be displayed, asking if you really want to do this.

Menu tab

Select the Menu tab to define the menu settings.

Click the Reset button to reset the menus to their original configuration.

Use the Context Menus dropdown menu to display any of the shortcut (or popup) menus: terminal shortcut menu, file transfer shortcut menu 1 (displayed when you do not have a file selected) or file transfer shortcut menu 2 (displayed when you have selected a file). Then you can click the Commands tab and drag menu options into the shortcut menus (and remove items from the shortcut menus by dragging them off the menu).

Use the Menu animation dropdown menu to select the type of menu animations. The available options are None, Unfold, Slide and Fade.

Select the Menu shadow check box to display shadows under open menus.

Options tab

Select the Options tab to change general user interface options.

Select the Show ScreenTips on toolbars check box to display a short help text, when you place the mouse pointer over a toolbar button.

Select the Show shortcut keys in ScreenTips check box to see the possible keyboard shortcut displayed in addition to the short help text.

Select the Large Icons check box to display big toolbar icons.

Select the Look 2000 check box to enable Windows 2000 style features in the user interface. This option has only minimal effects, and it affects mainly the style of toolbar handles.

Help

Click the Help button to display the online help.

Close

Click the Close button to stop the customization process.

Chapter 3

Connecting

SSH Secure Shell for Workstations Windows Client makes it easy to establish connections to new remote host computers, and to manage the settings required for each different host.

The Quick Connect option allows you to create new connections fast, minimizing the hassle associated with configuring each connection. It is easy to define a profile for new hosts, and save just the right settings for each.

3.1 Quick Connect

Select the Quick Connect option (from the toolbar or from the File menu) to establish a completely new SSH connection that can be operated independently of any other clients and connections. You can connect to an entirely new remote host computer and still keep the old connection to a different host open.

The Connect to Remote Host dialog will open, automatically filled in with the values defined in the default configuration file (`default.ssh2`). Therefore it makes sense to use the Settings dialog (see section 2.1 (Saving Settings)) to set the most commonly used options and save them in the `default.ssh2` configuration file.

When you need to establish a new connection, just click the Quick Connect button to connect to a new host with the default settings. When connected, you can then customize the settings to match your exact requirements for this particular host and save the settings as this host's profile (see section 3.2 (Profiles)).

But there is an even faster alternative. When you login using the default settings, the Add Profile dialog is briefly and non-intrusively shown. Click on the dialog and write in the name for the new profile. When you press the Enter key, the profile is automatically saved. It is accessible from the Profiles menu, and can later be fully customized.

3.2 Profiles

If you habitually connect to more than just one remote host computer, you probably want to have different settings defined for each host. Profiles make it easy to manage different host configurations.

You can have an unlimited amount of different profiles customized for different connections.

Note that the SSH Secure Shell for Workstations Windows client considers the profiles as the user's personal data and saves the profile definition files in the personal folder of the user. This means that every user of the local computer can have his or her own profiles, without affecting other users of the same computer.

Select the Profiles option (from the toolbar or the File menu) to either add a new profile definition or edit an already defined profile.

3.2.1 Add Profile

Adding a new profile is extremely easy. When you have connected to a new host computer, select the Add Profile option. The Add Profile dialog will open.

Figure 3.1: Just type in a name for the new profile and you are ready!

Type a name for the profile (the name of the host computer is a good choice) and press Enter. You are ready!

When you later want to connect to the same host, just select its profile under the Profiles option. You will be immediately connected, with all the settings in their proper places - even including the number and positions of SSH Secure Shell windows.

By using profiles, you can have just the right connection settings for each host, with no hassle or defining complicated configuration settings. It's that simple.

3.2.2 Edit Profiles

Click the Edit Profiles option to modify profiles that you have saved earlier. The Edit Profiles dialog will open, allowing you to edit all the host specific settings associated with this particular connection.

Click on the tabs on the top of the page to switch between pages. For a closer look on the settings displayed under each tab, see sections 2.4.1 (Connection), 2.4.2 (Authentication), 2.4.5 (Keyboard), 2.4.3 (Cipher List), 2.4.4 (Colors), and 2.4.7 (Tunneling).

You can make changes to several profiles at the same time by changing the profile with the profile tree displayed on the left hand side of the Edit Profiles dialog.

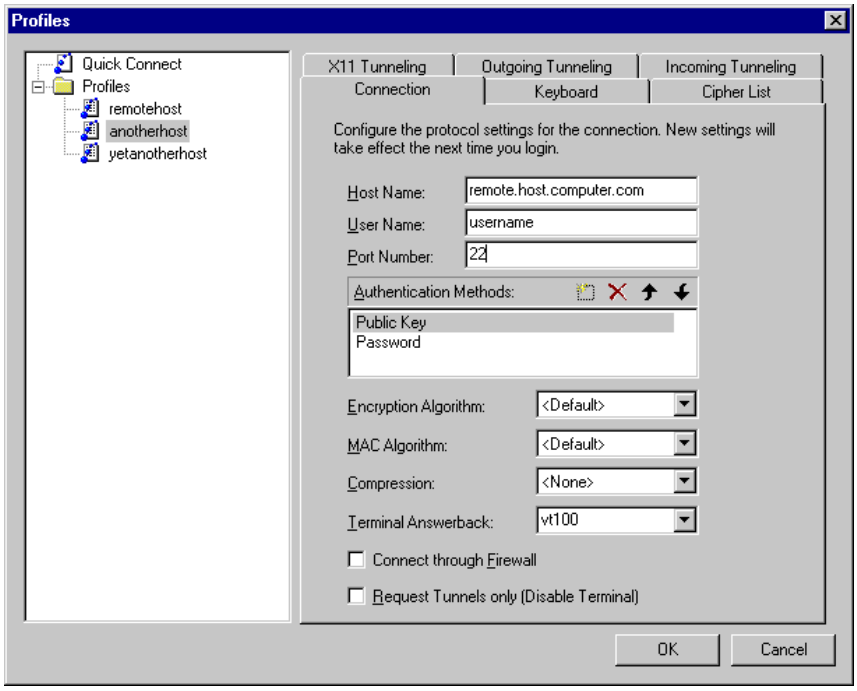

Figure 3.2: Use the Profiles dialog to customize settings for each host computer.

When you are finished with the settings, you can click the OK button to save the new profile definition, or the Cancel button to change your mind and abort your changes.

Note: Before the profile editing operation, the `.ssh2` settings are copied into backup files with the file extension `.bak`. If you remove these backup files, you will not be able to revert back to the old settings.

Profiles Shortcut Menu

Click the profile tree with the right mouse button, and a shortcut menu will open.

If you right-click on a profile, you can select from the following options:

Connect

Select the Connect option to immediately connect to the remote host computer associated with the profile.

Copy

Select the Copy option to copy the profile definition into the clipboard. Now you can click an empty location in the profile tree and paste a copy of the profile there.

Cut

Select the Cut option to remove the profile from its present location in the profile tree. Now you can click an empty location in the profile tree and paste the profile there.

Delete

Select the Delete option to remove the profile. A Confirm Delete dialog will open, asking if you are sure that you want to erase the selected profile.

Rename

Select the Rename option to type in a new name for the profile. It is a good idea to give each profile a descriptive name, so that the profiles are easy to recognize later on.

If you right-click on an empty spot on the profile tree, you can select from two options:

Paste

Select the Paste option to paste a profile that you have copied.

New Folder

Select the New Folder option to create a new folder in the profile tree.

Organizing Profiles

If you have defined a long list of profiles, it may be a good idea to organize them into folders. Click the profile list with the right mouse button, and select the New Folder option to create a new folder in the profile tree structure. Type a name for the new folder.

Now you can use the mouse to drag and drop the profiles and arrange them into folders so that you can quickly find the profiles you need.

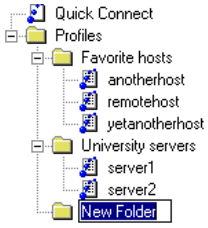

Figure 3.3: Creating a new folder for better organization.

3.3 Key Generation

If you are going to connect to a remote host computer using public-key authentication, you will have to generate your key pair before connecting.

Public-key authentication is based on the use of digital signatures. Each user creates a pair of 'key' files. One of these key files is the user's public key, and the other is the user's private key. The server knows the user's public key, and only the user has the private key.

When the user tries to authenticate herself, the server checks for matching public keys and sends a challenge to the user end. The user is authenticated by signing the challenge using her private key.

Remember that your private key file is used to authenticate you. Never expose your private keys. If anyone else can access your private key file, they can attempt to login to the remote host computer as you, and claim to be you. Therefore it is extremely important that you keep your private key file in a secure place and make sure that no one else has access to it.

Do not use public-key authentication on a computer that is shared with other users. Generate keys only on your personal computer that no one else can access!

In order to use public-key authentication, you must first generate your own key pair. You can generate your own key files with the help of a built-in key generation wizard.

3.3.1 Key Generation Wizard

To generate a new key pair, open the Settings dialog and select the User Keys page. Then click the Generate New Keypair button to run the key generation wizard.

The wizard will generate two key files, your private key and your public key. The private key file has no file extension, and the public key has the same base file name as the private key, but with .pub as the file extension. The key files will be stored in your local computer, in the user profile directory.

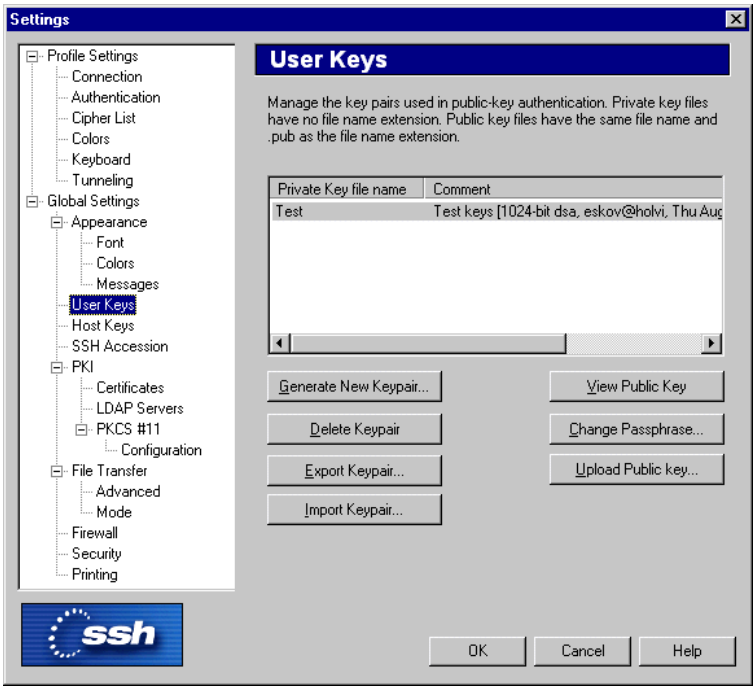

Figure 3.4: The User Keys page with a key pair already generated.

3.3.2 Key Generation - Start

The Key Generation - Start page contains important information about safety measures. Read the text and click the Next button.

Figure 3.5: The Start page of the key generation wizard.

3.3.3 Key Generation - Key Properties

On the **Key Properties** page, select the type of the key to be generated. You can select to generate either an RSA or a DSA key, as well as the key length. Larger keys are more secure, but also slower to use.

Key Type

Select the type of the key to be generated. Available options are DSA or RSA.

Key Length

Select the length (complexity) of the key to be generated. Available options are 768, 1024, 2048 or 3072 bits.

3.3.4 Key Generation - Generation

On the Key Generation - Generation page the computer will generate your key files. This can take several minutes, depending on the chosen key length and the processor speed of the computer.

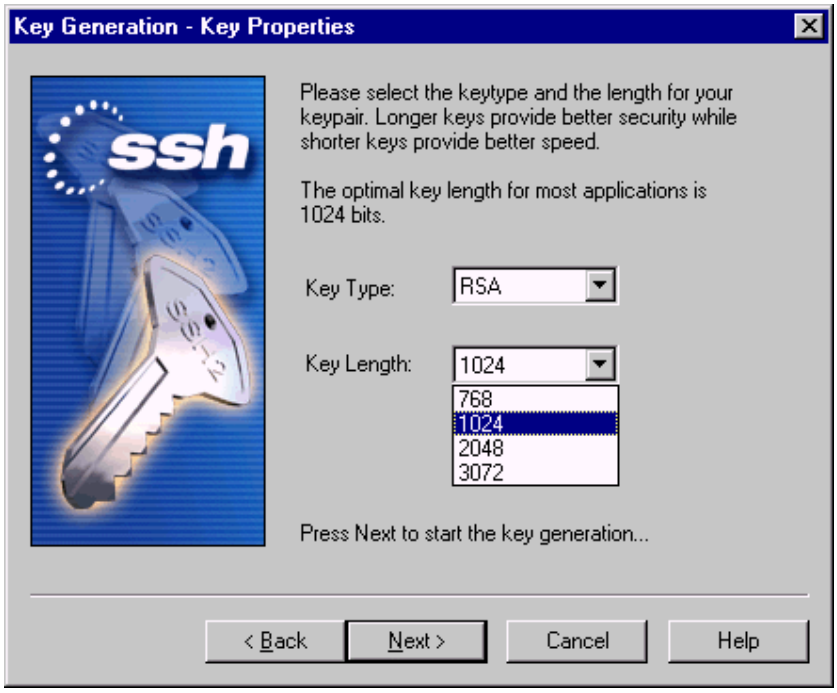

Figure 3.6: Selectin the key type

During the key generation phase an animation of random bits is displayed. When the process is ready, the Next button is ungrayed and you can proceed to the next phase by clicking it.

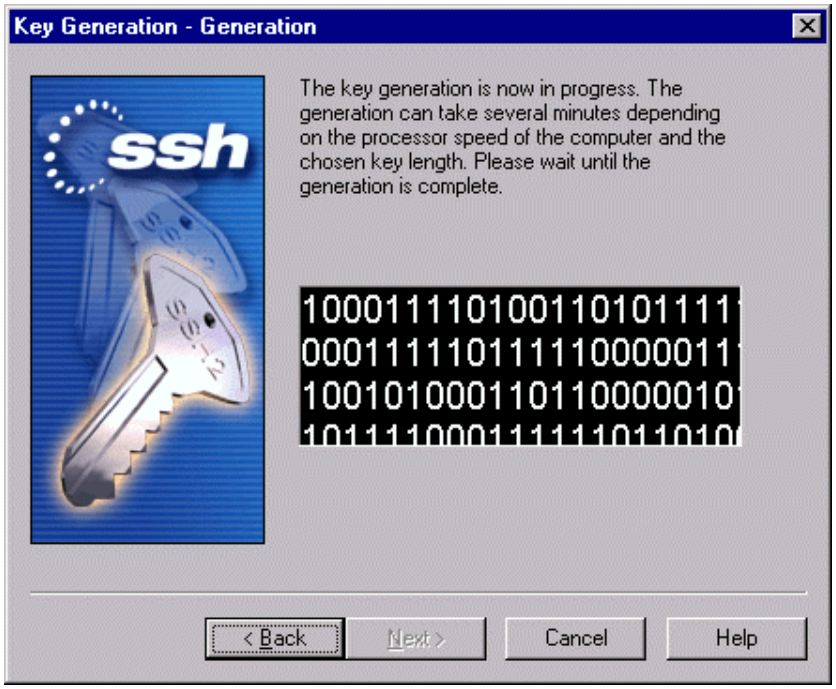

Figure 3.7: Key generation in process.

3.3.5 Key Generation - Enter Passphrase

On the Key Generation - Enter Passphrase page you can provide information describing the generated key pair, and protect the files with a passphrase.

Figure 3.8: Entering a passphrase for a newly generated key pair.

File Name

Type a name for the key file in the File Name field.

Comment

In the Comment field you can write a short comment that describes the key pair - you can for example describe the connection the files are used for. This field is not obligatory, but can be quite useful.

Passphrase

Type a phrase that you have to enter when handling the key. This passphrase works in a similar way to a password and gives some protection for your private key.

Make the passphrase difficult to guess. Use at least 8 characters, both letters and numbers. Any punctuation characters can be used as well.

Memorize the passphrase carefully, and do not write it down.

Passphrase

Type the passphrase again. This ensures that you have not made a typing error.

When you have typed in at least the file name and the passphrase (twice), you can click the Next button to proceed to the next phase.

3.3.6 Key Generation - Finish

The Key Generation - Finish page displays important information on the use of the key files.

The new public and private keys have been generated. They are currently stored on your local computer. To use these keys for public-key authentication, you have to upload the public keys to the remote host computer. If you are connected to a remote host, you can automatically have a copy of your new public key uploaded to the server by clicking on the Upload Public Key button. The public key file can be uploaded at a later date as detailed in the 3.5 (Uploading Your Public Key) section.

Click the Finish button to exit the key generation wizard.

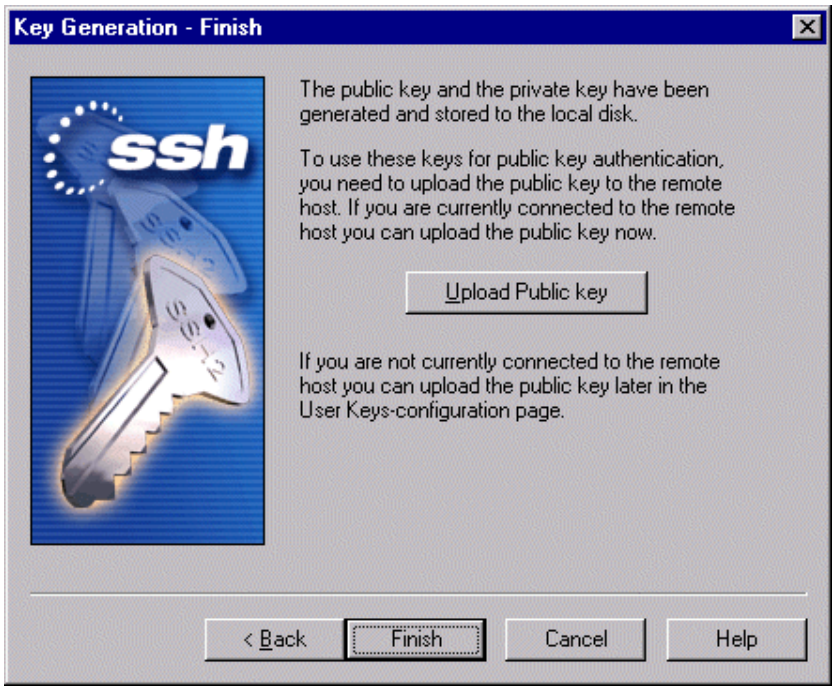

Figure 3.9: Keys have now been generated.

3.4 Connecting to a Remote Host Computer

To connect to a remote host computer, click the Connect icon on the toolbar, select the Connect option from the File menu, or just hit Enter or Space on the keyboard when the (still disconnected) client window is active. This brings up the Connect to Remote Host dialog.

When you connect to a remote host computer for the first time, the host will provide your local computer with a host public key. The host key is the public key for identifying the remote host computer that you're connecting to.

This process will bring up the Host Identification dialog.

3.4.1 Host Identification Dialog

When you connect to a remote host computer for the first time using public-key authentication, the host sends your local computer its public key in order to identify itself.

To help you to verify the host's identity, the Host Identification dialog displays a fingerprint of the host's public key. The fingerprint is represented using the SSH Babble format, and it consists of a pronounceable series of five lowercase letters separated by dashes. If you have reason to suspect that the public key you have received may be forged, you can for example phone the system administrator of the remote host machine and check if the fingerprint is correct.

If your work requires the strictest degree of absolute security and you cannot trust the network that was used to deliver the host key, you can ask the system administrator of the remote host computer to deliver the host's public key to you personally, for example on a diskette. This way the key is never passed over the network and you can be absolutely sure that it has not been forged. When using that host key with an SSH Secure Shell connection, you can be sure that you are connecting to the correct host and that there is no possibility of outside intrusion. However, for ordinary use this procedure can be seen as overkill.

The Host Identification dialog asks if you want to store the host key on your local computer. If you connect regularly to the host you will probably want to keep the key. This prevents an attack where someone can steal your connection.

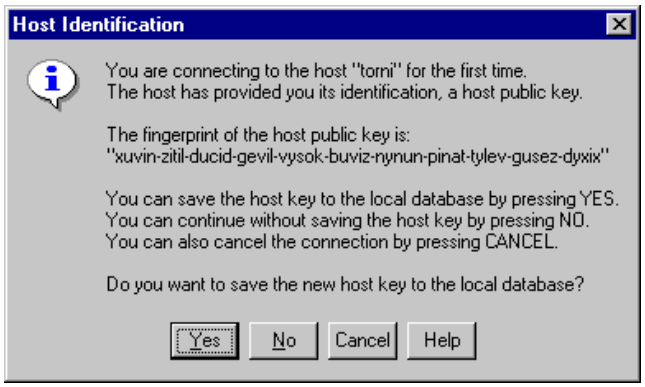

Figure 3.10: The Host Identification dialog.

Yes

You can save the host key to the local database by clicking Yes.

No

You can continue without saving the host key by clicking No. If you choose not to save the host key locally, you will be asked to the make this selection again next time you connect to this host.

Cancel

You can also cancel the connection by clicking on the Cancel button. This causes an authentication failure, and the connection will be canceled.

Help

Click the Help button to view the online help.

If you save the host key, you do not have to go through this procedure again the next time you login. The host's public key will still be checked with each connection, but this will be done automatically, without user intervention.

The known host keys will be saved in a local database that is specific to each user of the local computer. This way each user will build a personal database of the public keys of known and trusted hosts.

3.4.2 Connect to Remote Host Dialog

The Connect to Remote Host dialog allows you to specify the host name (or IP address), user name, port number and authentication method for the new connection.

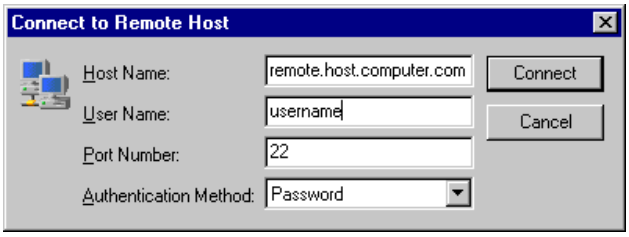

Figure 3.11: Identify yourself to the remote host computer.

The client remembers your previous connection. If you are going to reconnect to the same host, you do not have to type in all of the same information all over again.

Host Name

Enter the name (or IP address) of the remote host computer in this field. Unless this is your first connection, the Host Name field shows the name used in the previous connection. If you want to connect to the same computer as previously, you do not have to edit this field.

User Name

Enter your user name as used in the remote host computer. Unless this is your first connection, the User Name field shows the name used in the previous connection. If you want to connect using the same user name as previously, you do not have to edit this field.

Port Number

Type the number of the port used in the connection in the Port Number field. The port used in the previous connection is already filled in.

Authentication Method

Select the desired authentication method from the pulldown menu. Possible authentication methods are Password, Public Key, SecurID, PAM and <Profile Settings>.

Password

When you login using password authentication, you will have to type your password each time you establish a new connection to the remote host computer.

Public Key

Public-key authentication is based on the use of digital signatures. If you want to use public-key authentication, first you will need to create a pair of 'key' files (see section 3.3 (Key Generation)).

Before you can login using public-key authentication, you have to upload your public key to the remote host computer (see section 3.5 (Uploading Your Public Key)).

For more information on the use of public keys, see section 3.6 (Using Public-Key Authentication).

If you are using ssh protocol version 1 (ssh1) and want to authenticate using public keys, see the SSH Secure Shell FAQ (`http://www.ssh.com/faq/index.cfm?category=449`) for more information.

SecurID

Using SecurID authentication requires that you have a SecurID device that generates the numeric codes that are needed to login.

PAM

The Pluggable Authentication Modules (PAM) is an authentication method that has gained wide popularity especially on UNIX platforms.

<Profile Settings>

The authentication method specified in the active profile is used. The profile-specific authentication method can be defined using the Connection page of the Settings dialog (see section 2.4.1 (Connection)).

Connect

Click the Connect button to connect to the remote host computer.

Cancel

Click the Cancel button if you change your mind and want to abort the connection.

3.5 Uploading Your Public Key

If you want to use public-key authentication when connecting to the remote host computer, you have to upload your public key to the host. If you have not yet generated your own public key, see section 3.3 (Key Generation).

Public keys can be uploaded automatically to a server. After a connection has been made to a remote host, a User Keypair can be selected from the User Keys settings screen. Clicking on the Upload Public Key button will display the dialog box below before automatically uploading the public key to the specified directory and adding an entry for it to the `authorization` file.

If you do not use the automatic upload facility, you will need to place your public key file in the `.ssh2` subdirectory in your home directory on the remote host computer. The `authorization` file residing in the `.ssh2` directory must be edited to take the newly transferred key into use.

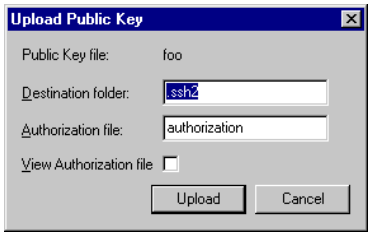

Figure 3.12: The Upload Public Key dialog.

Destination Folder

This is the subdirectory on the server where the public key file will be uploaded to. If this directory does not exist then it will be created under your home directory on the server. e.g. `~username/.ssh2`. The default value is `.ssh2`

Authorization File

This is the file on the server that contains details of your public keys. If this file does not exist then it will be created. The default value is `authorization`.

View Authorization File

Checking this box will allow you to view and edit the `authorization` file before it is uploaded to the server.

3.5.1 Manually Copying the Key File

The easiest way to manually copy your public key file is to open the Profile Settings page of the Settings dialog (select the Settings option from the Edit menu) and to click the Browse button next to the User Settings Folder field.

The folder containing your user settings is opened. The folder contains a subfolder called UserKeys. Double-click on the UserKeys folder to open it.

The folder containing your user keys is opened. Select the file that contains the public key that you want to copy to the remote host computer. Note that the public key has the file extension `.pub`. Be careful that you copy the file with the `.pub` extension, and not a similarly named file without a file extension (which would be your private key that you have to keep secure)!

Copy the file to the Windows clipboard by pressing `Control+C` on the keyboard, or by clicking the file icon with the right mouse button and selecting Copy from the shortcut menu.

Now connect to the remote host server and open a file transfer window, as described in chapter 5 (File Transfer).

Your home directory should contain a subdirectory named `.ssh2`. If you do not see the `.ssh2` directory, check that you have the Show Hidden Files option selected from the View menu.

Enter the .ssh2 directory and copy the key file there from the clipboard (press `Control+V` on the keyboard or click the right mouse button and select Paste from the shortcut menu).

3.5.2 Manually Editing the Authorization File

After you have uploaded your public key to the remote host computer, connect to the host using the SSH Secure Shell client's terminal window. Your home directory should contain a .ssh2 subdirectory (note that the first character of the folder name is a full stop).

First make sure that your current directory is your home directory. Type the following command after the remote host computer command prompt and press the Enter key:

```
cd
```

Then enter the .ssh2 subdirectory by issuing the following command after the command prompt:

```
cd .ssh2
```

The .ssh2 directory should contain a text file called `authorization`. You have to edit that file and add your public key file name on a separate line in that file. If the `authorization` file does not yet exist, you will create it now.

Start your favorite text editor by typing `authorization` as a parameter after the name of the text editor. For example, if your favorite text editor is Pico, type the following after the remote host computer's command prompt:

```
pico authorization
```

When in the text editor, add a new line containing the word `key`, a space and the public key file name. For example, if the public key file name is `public_key.pub`, add the following line to the `authorization` file:

```
key public_key.pub
```

Now save the `authorization` file and exit the text editor. When you login the next time, public-key authentication should be working. If it is not, check that you have typed the public key file name correctly in the `authorization` file, and that the correct public key file is located in the `.ssh2` directory on the remote host computer.

3.6 Using Public-Key Authentication

When you connect to a remote host computer using public-key authentication, you will first see the Connect to Remote Host dialog. When you hit the Enter key, public-key authentication will be attempted and if that fails the client will try password authentication.

If there is a suitable public key, the Enter Passphrase for Private Key dialog should be shown. This dialog indicates that the remote host computer is willing to accept your public key to authenticate you. If you do not see the Enter Passphrase for Private Key dialog, check that you have properly uploaded your public key, as described in section 3.5 (Uploading Your Public Key).

Type in the passphrase associated with this key. You defined the passphrase when you create the public key - see section 3.3.5 (Key Generation - Enter Passphrase) for more information.

(If you again just press the Enter key, the key will not be used and the system will ask your password instead.)

If you enter the correct passphrase, you will connect to the remote host computer.

Note that in some cases the remote host computer may be configured to use both public-key authentication and password authentication for increased security. In that case you will first have to type in your password, and after that to also use public key authentication.

The authentication sequence above assumes that the client is configured to use any authentication method (see section 2.4.2 (Authentication Methods)).

3.7 Command Line Options

For some purposes it may be useful to operate the SSH Secure Shell for Workstations Windows Client from the command line (command prompt).

The SSH Secure Shell client command line syntax is:

```
sshclient [-r] [-p port] [-u user] [-h host] [profile.ssh2]
```

The following command line options can be used to define the connection parameters:

-r

The -r option will reset all customizations made to the user interface (toolbars and menus). A confirmation dialog will be displayed.

-p [port_number]

The -p option specifies the port number used for the connection. If this option is not specified, the port number defined in the default profile will be used.

-u [user_name]

The -u option specifies the user name for the connection. If this option is not specified, the user name defined in the default profile will be used.

-h [host_name]

The -h option specifies the host name for the connection. If this option is not specified, the host name defined in the default profile will be used.

[profile.ssh2]

If a profile is specified, it must the last option on the command line. Any command line parameters will override the profile settings. If no profile is specified, the default profile (`default.ssh2`) will be used.

For example, the following command would immediately start a connection to a host called remotehost and connect as guest. The port number is not specified, so the connection would use the port specified in the default profile.

```
sshclient -h remotehost -u guest
```

The following command would immediately start a connection to remotehost using the settings defined in the profile file `custom.ssh2`.

```
sshclient -h remotehost custom.ssh2
```

If the host is not specified (using the -h option) and no profile is specified, the login dialog will open, automatically filled with the values specified on the command line.

For example, the following command would display the login dialog with the port number already defined as 222 and the user name as guest.

```
sshclient -u guest -p 222
```

Several other command line utilities are shipped with the Windows client. For more information, see the appendices section (A (Appendices)).

Chapter 4

Terminal Window

The terminal window is a secure replacement for Telnet connections. It offers a command line interface to the remote host computer. Note that the most important function of the terminal window is to allow you to operate the remote host computer. Therefore the terminal window does not capture some common keyboard shortcuts (such as `Ctrl+C` for copy), but passes them instead to the remote host computer, where they can be used to control remote program execution.

Apart from the text display itself, a lot of connection information is visible in title and status bars of the Terminal window.

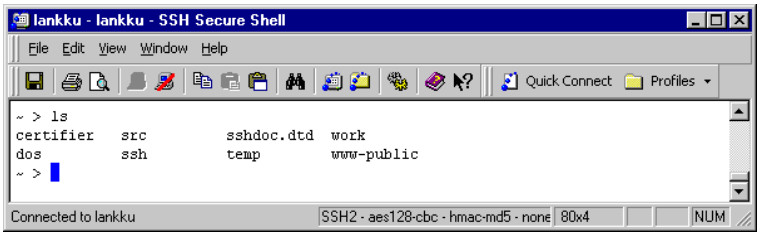

Figure 4.1: The Terminal window.

4.1 Terminal Window Title Bar

The title bar is located on the top of the window.

The leftmost item on the title bar is the window icon. Click it to display the Window menu or doubleclick it to close the window.

The next item on the title bar is the window's sequence number. This helps you to distinguish between different windows using the same connection.

Next on the title bar is displayed the remote computer's host name. For example, a second window associated with a connection to a host computer called remote would display as `2:remote`.

After the host name, the next item on the title bar is the name of the settings file in use. If you are not using a settings file that has been saved with a specific file name (using the Save As option on the File menu), a settings file called `default` is in use.

The last text item on the title bar is the name of the client, SSH Secure Shell.

4.2 Terminal Window Status Bar

The status bar is located at the bottom of the Terminal window. When browsing through the menu options or toolbar buttons, the status bar displays a short context sensitive help text.

When the menus or toolbars are not browsed, the left side of the status bar indicates to which remote host computer you are currently connected. If you are not connected, the status bar displays the text `Not connected - Press Enter/Space to connect`.

The next status bar field shows the current protocol version, encryption algorithm, and MAC algorithm separated by dashes (for example: `ssh2 - 3des-cbc - hmac-md5`). Note that the status bar displays some of the algorithm names in a longer form than the Connection screen of the Settings dialog.

The next field displays the number of columns and rows of the terminal window. If you change the size of the terminal window, this window size indicator will be immediately updated.

If you have a smart card reader active, you should see a small card reader icon on the next column of the status bar. When a token is inserted, a smart card appears in the card reader in the icon. When a key is acquired from the token, a key symbol appears on top of the card reader icon. If the icon does not appear, see section 2.5.14 (PKCS 11 Provider) for troubleshooting information.

The next field displays the text `CAP` if your Caps Lock key is currently on.

The last field of the terminal window status bar displays the text `NUM` if your Num Lock key is currently on.

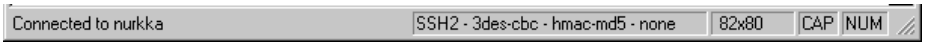

Figure 4.2: Terminal window status bar.

4.3 Terminal Window Shortcut Menu

Click the terminal window with the right mouse button to display a shortcut menu. By default, the following menu options are available:

Copy

Copy text into the Windows clipboard.

Paste

Paste text from the Windows clipboard.

Paste Selection

Copy the currently selected text into the cursor location without first copying it into the Windows clipboard.

Select All

Select all of the scrollback buffer.

Select Screen

Select all text currently displayed on the screen. The rest of the scrollback buffer will not be selected.

Select None

Cancel the current selection.

Find

Search for text from the scrollback buffer.

New Terminal

Open a new terminal window.

New File Transfer

Open a new File Transfer window.

Close Window

Close the current window.

Settings

Open the Settings dialog.

The available options can be configured using the Customize dialog (see section 2.6 (Customize)).

Chapter 5

File Transfer

SSH Secure Shell makes it easy and convenient to transfer files between your local computer and the remote host computer. You can upload and download files by using an intuitive, graphical user interface similar in functionality to the Windows Explorer.

You can open the File Transfer window by clicking on the New File Transfer Window button on the Secure Shell toolbar, or by selecting the New File Transfer option from the Window menu. You can have an unlimited number of individual File Transfer windows open at the same time.

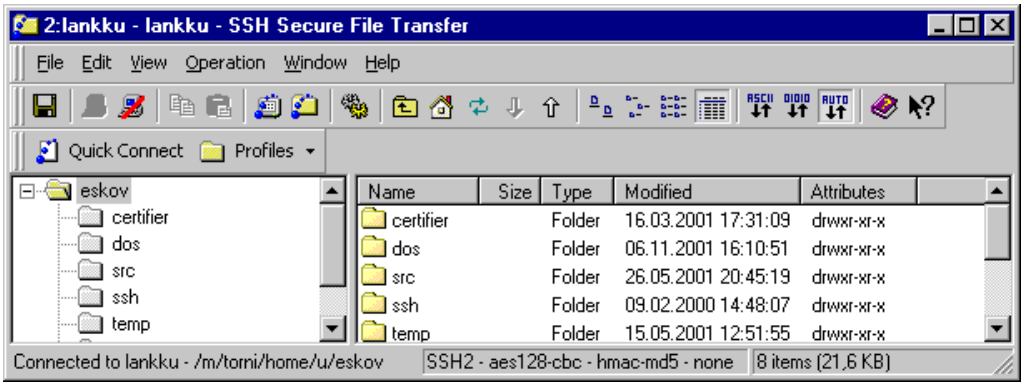

Figure 5.1: The File Transfer dialog.

The Secure Shell 2 File Transfer contains several unique features that make secure transfer operations fast and easy.

Note, however, that the SSH Secure Shell for Workstations Windows client is not just an alternative to an FTP client. You cannot for example use the ssh2 client to login to a normal, insecure FTP host. The remote host computer must be running an ssh2 server.

Please note that the maximum size of a transferred file depends on the limitations of the file system.

5.1 Drag And Drop Operations

You can use drag and drop mouse operations to copy and move files to and from the remote host computer.

This works in a similar fashion to the standard Windows drag and drop operations. If you hold down the Shift or Control keys when selecting files with the mouse, you can select multiple files and copy them all at the same time. If you hold down the Shift key, all the files and folders between the first and last selection will be selected. If you hold down the Control key, you can select individual files and folders one by one.

If you doubleclick a file, the file will be opened by using a custom application. (Notepad will be used by default.) For more information on specifying the custom application, see section 2.5.15 (Missing File Association).

5.2 Folder View

The directory structure of the remote host computer is visible on the left hand pane of the File Transfer window. The directory structure is presented as a tree-like folder structure, familiar from the Windows Explorer.

Folders that have a plus sign (+) next to them can be opened by clicking on the plus sign. Open folders have a minus sign (-) next to them and can be closed by clicking on the minus sign.

You can click on a folder to view its contents on the right hand side pane of the File Transfer window. The displayed folder shows up highlighted on the folder view.

Opening or closing a folder in the folder view does not affect the file view on the right hand side, unless you close the displayed folder's parent folder. In that case the closed folder becomes the new displayed folder.

5.2.1 Folder Colors

To make file transfer operations easier, the folders in the remote host computer are displayed in different colors according to their status.

Yellow folders are 'familiar folders' that are known to be available for your use. Usually this means that you have opened them earlier.

Gray folders are 'unknown folders' that have not yet been visited. Therefore the SSH Secure Shell for Workstations Windows client does not yet know if the remote host computer allows you to access them.

Red folders are 'forbidden folders'. You don't have a permission to access them, and therefore the remote host computer does not allow you to view their contents. If you select a red folder, the File view on the right will be blank. Select some other folder to continue.

Green folders are 'folders being loaded'. When you select a new folder, it turns green for the time it takes to list its contents. Unless the folder contains a large number of files and subfolders (or the connection is slow), the folder does not stay green longer than a fraction of a second.

5.3 File View

The files in the currently open folder are displayed on the File View pane on the right hand side of the File Transfer window. If you have not yet opened any folders, the initial view shows the files in your 'home directory' on the remote host computer.

You can open folders visible in the File View pane by clicking them the same way as in the Folder view.

You can move in the directory tree also by clicking the Parent Directory button in the toolbar, or by pressing the Backspace key on the keyboard. This moves the view from the current directory to its parent directory.

The file icons and file type descriptions are derived from the client computer. If you have a specific icon associated with a certain file type, the files in the host computer show up with the familiar icon. This makes it faster and easier for you to recognize files of different type.

You can use the Tab key to switch between the folder view and the file view.

5.4 File Transfer Title Bar

The title bar is located on the top of the window.

The leftmost item on the title bar is the window icon. Click it to display the Window menu or doubleclick to close the window.

The next item on the title bar is the window's sequence number. This helps you to distinguish between different windows using the same connection.

Next on the title bar is displayed the remote computer's host name. For example, a second window associated with a connection to a host computer called remote would display as `2:remote`.

After the host name, the next item on the title bar is the name of the settings file in use. If you are not using a settings file that has been saved with a specific file name (using the Save As option on the File menu), a settings file called `default` is in use.

The last text item on the title bar is the name of the client, SSH Secure Shell File Transfer.

5.5 File Transfer Status Bar

The status bar is located at the bottom of the File Transfer window. When browsing through the menu options or toolbar buttons, the status bar displays a short context sensitive help text.

Figure 5.2: The File Transfer status bar displaying the size of a selected file.

When the menus or toolbars are not browsed, the left side of the status bar displays the current remote host computer and the path in the remote host.

The next status bar field shows the current protocol version, encryption algorithm, and MAC algorithm separated by dashes (for example: `ssh2 - 3des-cbc - hmac-md5`). Note that the status bar displays some of the algorithm names in a longer form than the Connection screen of the Settings dialog.

The rightmost field of the File Transfer status bar displays the number of files and subfolders in the current folder, as well as the total size of the files. If you select file(s) in the folder view, the field changes to display the number and total file size of the current selection. This is especially useful when estimating the amount of total data to be transferred.

5.6 File Transfer Shortcut Menu

Click the File Transfer window with the right mouse button to display a shortcut menu. The available menu options depend on whether you have selected a file or not.

The following menu options are available when you have not selected a file:

Paste

Paste a file from the File Transfer 'clipboard'.

Upload

Transfer a file from the local computer into the remote host computer.

Up

Move the File Transfer window focus into the parent directory of the current directory.

Home

Move the File Transfer window focus into your home directory.

Go to Folder

Opens the Go to Folder dialog where you can type in a path of the folder which you want to open.

Refresh

Redraw the File Transfer window.

Select All

Select all files and folders in the current folder.

View

Opens a submenu from which you can select the view type (large icons, small icons, list or details view).

Arrange Icons

Opens a submenu from which you can select how the icons are arranged (by name, by type, by size or by date).

New Folder

Creates a new folder and prompts you to enter a name for it. If you enter nothing, the folder will not be created.

The following menu options are available when you have selected a file or folder:

Open

Open the currently selected file or folder.

Copy

Copy the currently selected file into the File Transfer 'clipboard'.

Download

Transfer the currently selected file into the local computer.

Delete

Remove the currently selected file.

Rename

Change the name of the currently selected file.

Properties

Display the attributes of the currently selected file, including the file permissions (on UNIX systems).

The available options can be configured using the Customize dialog (see section 2.6 (Customize)).

5.7 Differences From Windows Explorer

The File Transfer window operates very much the same way as the familiar Windows Explorer. However, due to the different nature of handling files locally in your own computer (as per Windows Explorer) and handling them over a secured remote connection in the host computer (as per SSH Secure Shell for Workstations Windows client File Transfer), there are some differences in operation.

Deleting folders

It is not possible to delete a remote folder that is not empty. Delete the files and subfolders residing in the folder first.

Multiple paste operations

During copy and paste operations, the file names are not changed when the files are pasted. Therefore it is not possible to paste files several times into one location, creating 'copies of' the pasted files as in Windows Explorer.

5.8 Downloading Files

By using the File Transfer window it is easy to download files from the remote host computer into your local computer. There are several different ways to download a file - or several files at the same time.

To select multiple files, hold down the Shift or Control keys when selecting files with the mouse. If you hold down the Shift key, all the files and folders between the first and last selection will be selected. If you hold down the Control key, you can select individual files and folders one by one.

Drag and drop

Dragging and dropping is probably the easiest way to download files. Simply click on the file(s) you want to download, hold down the mouse button and move the file to a location where you want it - for example on the Windows desktop - and release the button.

Download button

You can click the Download button on the toolbar to download the selected file(s).

Shortcut menu

When you click a file or folder using the right mouse button, a shortcut menu appears. The shortcut menu shows the most common file operations: open, copy, download, rename and delete. Select the desired operation from the menu, and it will be applied to all of the currently selected files or folders.

When the download starts, a Download - Select Folder dialog will appear, allowing you to select where the downloaded file(s) should be saved. After you have selected the appropriate folder (or other location), you will see a Downloading dialog that shows the current downloading status.

5.8.1 Download - Select Folder Dialog

When you start a download operation, a Download - Select Folder window is displayed. This is a standard Windows file selection dialog, where you can select the location where you want the selected file(s) to be downloaded.

You can use the Look in selection box to select a folder, a local or network drive or your desktop. Note: Transferring files to or from a network drive is not supported on Windows 95.

Another way to select the desired folder is to type its directory path in the Folder field. Note that you can use this field only to specify the folder name. Do not write in a file name after the selected directory path. The file name will be the same the file has in the remote host computer.

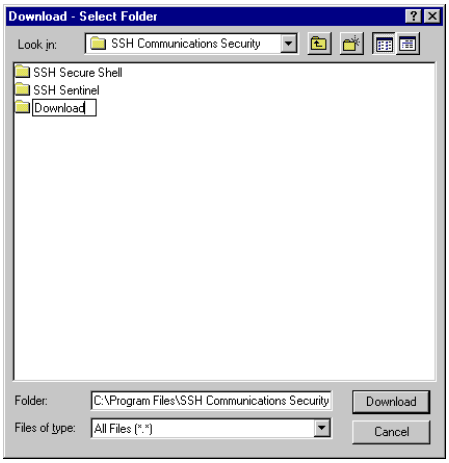

Figure 5.3: Creating a new directory for downloaded files.

The most common operations can be achieved by clicking on the four buttons on the right hand side of the Look in selection box. You can click on the Up One Level button to move to the parent folder of the current folder. If you want to create a new folder, click on the Create New Folder button. You can also select between the Small Icons and Details views by clicking on the appropriate buttons.

5.8.2 The Downloading Dialog

The Downloading dialog displays the current status of download.

At the top of the dialog a familiar file copy animation indicates a transfer in progress. The progress bar below the file copy animation shows the approximate percentage of how much of the current file transfer has been completed.

A more exact figure is displayed on the Transferred field below the progress bar. The Transferred field displays how much of the file has currently been transferred and what is the total file size.

The Transfer Rate field shows the current rate of transfer (how many kilobytes of data are being transferred per second).

The message area, located below the Transferred and Transfer Rate fields, displays the transferred files and their sizes. Also any informational or error messages are displayed there.

When the download is complete, the title of the Downloading window changes into Download Complete. Click the Close button to close the dialog and return to the File Transfer window.

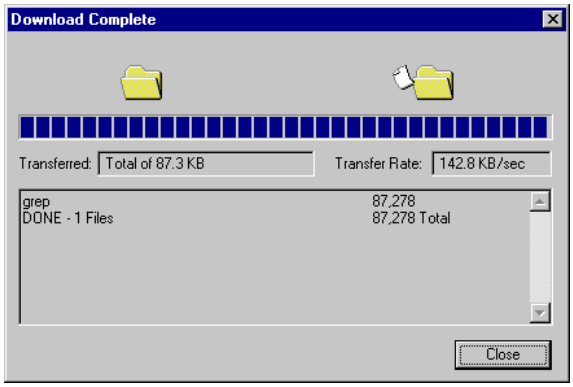

Figure 5.4: The download has been completed.

5.9 Uploading Files

The File Transfer window can be used to upload files from your local computer to the remote host computer. There are several different ways to upload a file.

It is also possible to upload several files at the same time. To select multiple files, hold down the Shift or Control keys when selecting files with the mouse. If you hold down the Shift key, all the files and folders between the first and last selection will be selected. If you hold down the Control key, you can select individual files and folders one by one.

Drag and drop

Dragging and dropping is probably the easiest way to upload files. Simply click on the local file(s) you want to upload (for example on the desktop or the Windows Explorer), hold down the mouse button, move the file(s) into the File Transfer window's file view and release the button.

Upload button

You can click the Upload button on the File Transfer window's toolbar to upload the selected file(s).

Shortcut menu

When you click on an empty space in the File Transfer window's file view using the right mouse button, a shortcut menu appears. The shortcut menu allows several file transfer operations: Paste, Upload, Up, Home, Go To Folder, Refresh, Select All, View, Arrange Icons and New Folder. Select the desired operation from the menu.

When the upload starts, a Upload - Select Files dialog will appear, allowing you to select the file(s) that should be uploaded. After you have selected the file(s), click the Upload button. You will see a Uploading dialog that shows the current uploading status.

5.9.1 Upload - Select Files Dialog

When you start an upload operation, a Upload - Select Files window is displayed. This is a standard Window file selection dialog, where you can select which file(s) you want to upload.

You can use the Look in selection box to select the location of the file(s): a folder, a local or network drive or your desktop.

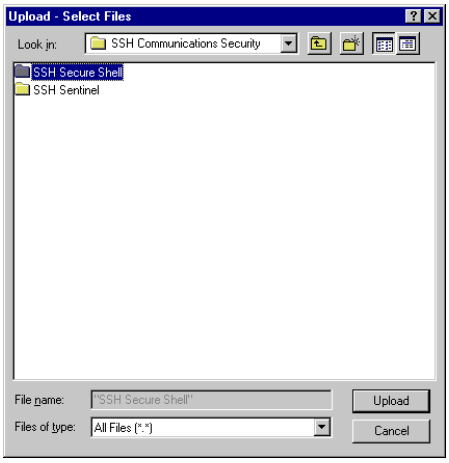

Figure 5.5: Select the file you want to upload.

Note that the File name field displayed at the bottom of the dialog displays the selected file name. The field is read-only - you cannot type in the desired file name. Select the files by clicking them with the mouse instead.

The most common operations can be achieved by clicking on the four buttons on the right hand side of the Look in selection box. You can click on the Up One Level button to move to the parent folder of the current folder. If you want to create a new folder, click on the Create New Folder button. You can also select between the Small Icons and Details views by clicking on the appropriate buttons.

5.9.2 The Uploading Dialog

The Uploading dialog displays the current uploading status.

At the top of the dialog a familiar file copy animation indicates a transfer in progress. The progress bar below the file copy animation shows the approximate percentage of how much of the current file transfer has been completed.

A more exact figure is displayed on the Transferred field below the progress bar. The Transferred field displays how much of the file has currently been transferred and what is the total file size.

The Transfer Rate field shows the current rate of transfer (how many kilobytes of data are being transferred per second).

The message area, located below the Transferred and Transfer Rate fields, displays the transferred files and their sizes. Also any informational or error messages are displayed there.

When the upload is complete, the title of the Uploading window changes into Upload Complete. Click the Close button to close the dialog and return to the File Transfer window.

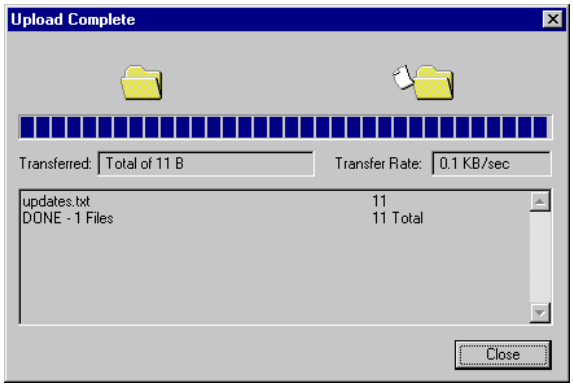

Figure 5.6: A file has been uploaded.

5.10 File Properties

Selecting a file in the File View window then selecting the Operation, Properties menu option brings up the File Properties page which allows you to view and change some of the remote files properties. The Properties page can also be accessed by right clicking on a file in the File View pane and selecting Properties.

File Name

At the top of the page the file name and icon are shown. If multiple files are selected, a count of the number of files and folders is displayed.

Type

The type of the selected file(s).

Location

The directory where the selected file(s) are located on the remote host.

Size

The size of the selected file. If multiple files are selected the total size of all the files is diplayed.

Modified Date

The last modified date for the selected file.

Permissions

The 9 check boxes can be used to set the permissions of a file or a group of files. If multiple files are selected with conflicting permissions then some of the check boxes will appear grayed out. Clicking

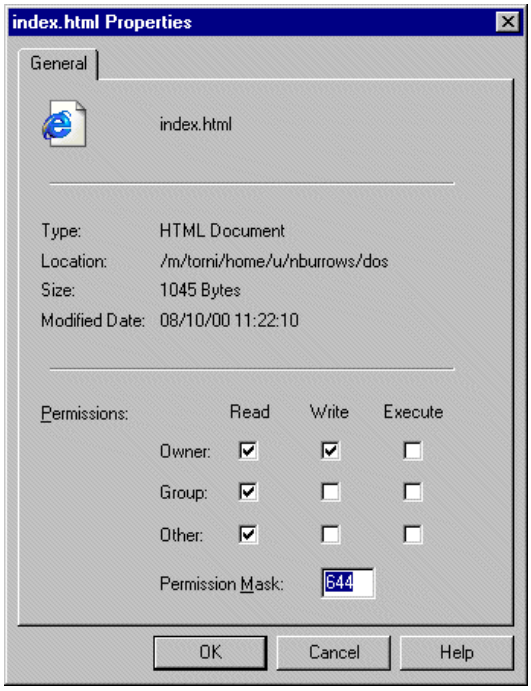

Figure 5.7: Properties page for a file.

on a greyed out check box will clear the check mark. If there are any check boxes are grayed out when the OK button is pressed it will have the effect of leaving that value unchanged on the remote file.

Permissions can also be set by entering standard octal UNIX permission masks (as with the `chmod` command) in the Permission Mask field. Values entered here override and update the check box values.

Chapter 6

Toolbar Reference

The most important functions of the SSH Secure Shell for Workstations Windows client's terminal window and File Transfer window can be accessed using the *toolbar*. By default the toolbar is located at the top of the SSH2 client window, right under the menubar.

Figure 6.1: The basic toolbar contains buttons for the most frequently used functions.

By default the profiles toolbar is located under the basic toolbar, containing the Quick Connect and Profiles options.

Figure 6.2: The profiles toolbar contains the Quick Connect and Profiles buttons.

6.1 Configuring Toolbars

The SSH Secure Shell for Workstations Windows client has a dynamic user interface that is very easy to modify to match to your tastes. You can select the position of the toolbars, and even move individual buttons from one place to another.

6.1.1 Moving Toolbars

You can use the mouse to grab the toolbars by their handles (located on the lefthand end of each toolbar) and move them around the SSH Secure Shell window.

You can have the toolbars floating freely in the window, or anchor them in the top, bottom or even either side of the window. Experiment to find the toolbar positions that you like best.

6.1.2 Moving Toolbar Buttons

You can also move individual toolbar buttons around and arrange them so that they best serve your needs.

To move a toolbar button, keep the `Alt` key on the keyboard pressed down and grab a button with your mouse. You will see a new mouse pointer appear. Click the button with your left mouse button, keep the mouse button pressed down and move the button around. When you release the mouse button, the toolbar button will be move to a new position.

Note: If you move a button to somewhere else than a toolbar (for example, in the terminal window text area), it is removed from the window. But don't worry - the changes become permanent only if you use the Save Settings option (see section 6.2 (Save Settings)).

6.1.3 Permanent Toolbar Changes

If you want to make the new toolbar positions permanent, use the Save Settings option (from the toolbar or the File menu) to save your settings.

If you change your mind and want to return the toolbars to their original positions, select the Reset Toolbars option from the View menu. A confirmation dialog will open, asking if you really want to discard the changes you have made. If you select Yes, the toolbars will return to their original configuration. If have modified your menus, this option will reset also them.

6.2 Save Settings

Select the Save Settings option to save any changes you have made to your current settings. The default settings file where the configuration will be saved is `default.ssh2`.

If you want to save your current settings in a new settings file, select the Add Profile option under the Profiles option (see section 3.2 (Profiles)).

6.3 Print

Select the Print option to output the contents of the current scrollback buffer to your printer. The standard Windows Print dialog will appear, allowing you to select the printer settings.

The print range can also be selected from this dialog. Selecting All will print the entire contents of the terminal scrollback buffer. If the whole scrollback buffer will fill more than one page when printed, a range of pages to print can be selected. If any text is selected when you use the Print option, the default print range will be Selection, which will only print the currently selected text.

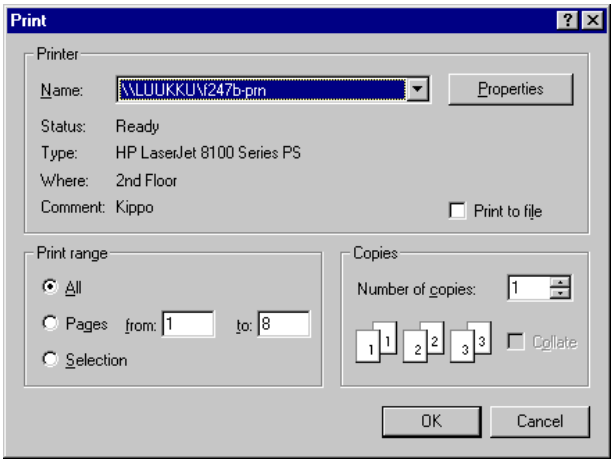

Figure 6.3: The Print dialog allows you to specify the printer settings.

You can use the Print Preview option (see section 6.4 (Print Preview)) to help you to determine which pages to print and how the printout will look like.

Note: when you use a network printer, the area selected for printing will be sent unencrypted over the network to the printer.

The Print option is available only in the terminal window.

6.4 Print Preview

Select the Print Preview option to display the entire contents of the terminal scrollback buffer, split into pages in the same way as the scrollback buffer will appear when printed.

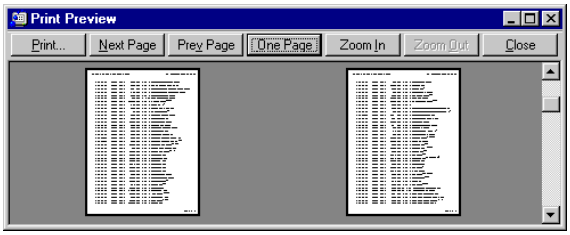

Figure 6.4: The Print Preview option show the scrollback buffer as it would appear when printed.

The following buttons can be used to preview the print result:

Print

The Print button opens the Print dialog, allowing you to specify the printer settings and print the result.

Next Page

Click the Next Page button to preview the next page of output. The keyboard shortcut for Next Page is the `Page Down` key.

Prev Page

Click the Prev Page button to preview the previous page of output. The keyboard shortcut for Prev Page is the `Page Up` key.

One Page / Two Pages Toggle

Click the One Page / Two Pages Toggle button to display two pages of output side by side. When in two page print preview mode, the Two page button is replaced by One Page button, which allows you to return to the one page print preview mode. This button cannot be used when you have zoomed the page.

Zoom In

Click the Zoom In button to see a closeup of the currently displayed print preview page. You can use this button to zoom up to the natural size of the printout. You can zoom in also by clicking the left mouse button on the preview view.

Zoom Out

Click the Zoom Out button to return from a zoomed in view of the print preview page. You can zoom out until the whole page is displayed.

Close

Click the Close button to close the Print Preview dialog. The dialog can be closed also by pressing the `Esc` key.

The Print Preview option is available only in the terminal window.

6.5 Connect

Select the Connect option to connect to a remote host computer. A Connect to Remote Host dialog will open.

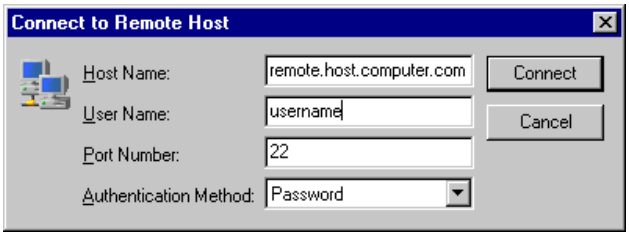

Figure 6.5: The Connect to Remote Host dialog.

For more information on this dialog, see section 3.4.2 (Connect to Remote Host Dialog).

6.6 Disconnect

Select the Disconnect option to quit the current connection. A **Confirm Disconnect** dialog is displayed, allowing you to confirm if you really want to disconnect. Select **No** or **Cancel** to keep the connection open, or **Yes** to end the connection. If you do not want to see the Disconnect confirmation dialog again, select the **Do not ask this question again** check box.

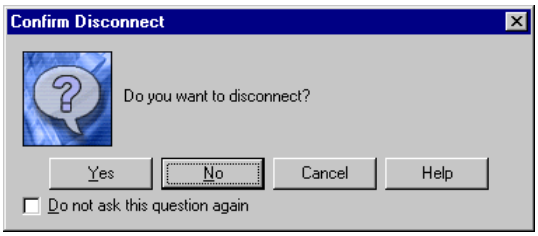

Figure 6.6: The Confirm Disconnect dialog gives you the last change option of changing your mind.

Note that one connection can have several windows open (such as an SSH Secure Shell for Workstations Windows client terminal window and a File Transfer window). Disconnecting affects all windows associated with a single connection.

However, if you have started other, separate SSH Secure Shell for Workstations Windows clients, they are not affected by this disconnect operation. Disconnecting quits one connection and all of its associated windows, but no other, separate connections.

6.7 Copy

Select the Copy option to create a temporary copy of the selected text or files.

If you are copying text (in the terminal window), the text is placed on the Windows clipboard and can be pasted in the terminal window or any Windows text window.

If you are copying files (in the File Transfer window), a Download dialog is displayed, but the selected files are not yet copied to any specific location. This resembles using the Windows clipboard: You can copy files to a temporary storage and paste them later into another location.

If you do a new copy operation when the previously copied text or files have not yet been copied anywhere, the previous selection is lost, as the new selection replaces the old one.

Note that the copy option is not available until you have selected some text (in the terminal window) or one or several files or folders (in the File Transfer window).

You can do a copy operation also by using the keyboard shortcut `Ctrl+Insert`. This shortcut is available in both Terminal and File Transfer windows.

6.8 Paste

Select the Paste option to add previously copied text or files or folders into a new location.

If you are pasting text (in the terminal window), the text that was copied earlier into the clipboard will be inserted in the cursor location. You can paste text that was copied from the terminal window or any other Windows text window.

If you are pasting files (in the File Transfer window), an Upload dialog is displayed when the files are pasted to the new location. This resembles using the Windows clipboard: You can copy files to a temporary storage and paste them later into another location. The file names of the pasted files and folders do not change during the operation. Therefore it is not possible to paste files or folders several times into one location.

Note that the paste operation is not available until you have previously copied something in the clipboard.

You can do a paste operation also by using the keyboard shortcut Shift-Insert on the keyboard. This shortcut is available in both Terminal and File Transfer windows.

6.9 Paste Selection

Select the Paste Selection option to paste text into the terminal window without first copying anything to the clipboard. The Paste Selection operation copies whatever is currently selected in the terminal window to the present cursor position. If no text is selected, Paste Selection pastes the single character in the current cursor position.

This function is almost like having two different clipboards available at the same time. Paste Selection is especially useful for quick copying of text from the output of previous commands.

The Paste Selection toolbar button is available only in the terminal window.

6.10 Find

Select the Find option to locate text (or any other characters) from the scrollback buffer. Regular expressions can be used to select characters matching a specific pattern.

Find what

Type in the characters that you want to search for in the Find what field. If you want to use regular expressions to define the search term, select the Regular expression option, or select a ready defined regular expression by clicking the ellipsis button (...) on the right hand side of the Find what field.

...

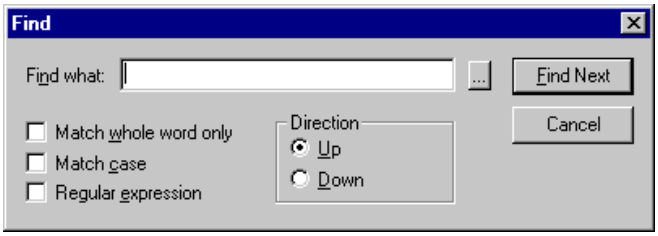

Figure 6.7: The Find dialog helps you to locate text from the scrollback buffer.

Click the ellipsis button (...) to select from a ready list regular expressions. Using this option will turn on the Regular expression option.

The following regular expression types can be selected:

Any Character

Character in Range

Character not in Range

Beginning of Line

End of Line

Or

0 or More Matches

1 or More Matches

Optional Match

Match exactly n times

Match n or more times

Match at most n times

Match no less than n times and no more than m times

Match whole word only

Select the Match whole word only option to limit the search to match only whole words (i.e. so that ”wave” would not match ”waves”).

Match case

Select the Match case option to specify that the search result should be case sensitive (i.e. so that ”Wave” would not match ”wave” or ”waVe”).

Regular expression

Select the Regular expression option to specify the search term using regular expressions. This option is automatically selected if you click the ellipsis button (...) on the right hand side of the Find what field.

Direction

Use the Direction option to specify whether the search should start upwards on downwards from the present position in the scrollback buffer.

The direction of the search is relative to the last match made in the current search. If there have been no previous matches, Up will search from the bottom of the buffer upwards, and Down will search downwards from the very beginning of the buffer.

Up

The Up option specifies that the search should start backwards from the present position.

Down

The Down option specifies that the search should start forward from the present position.

Find Next

Click the Find Next button to find the next match for the search term. Note that the direction where the search will continue is defined by the Direction option.

Cancel

Click the Cancel button to close the Find dialog.

6.11 New Terminal Window

Select the New Terminal Window option to open a new SSH Secure Shell for Workstations Windows client terminal window. The new window is immediately connected to the same remote host computer as the current window, saving you the trouble of typing your password again.

Multiple windows to a single connection allow you to for example debug your code in one window, execute it in another, display reference information in a third one and read your mail in a fourth window.

The sequence number of each window is displayed on the window's title bar, in front of the remote host computer's name. For example, a second window associated with a connection to a host computer called remote would display as `2:remote`.

Note: To close any extra windows when you no longer need them, click on the X-shaped close button located on the window's title bar on the upper right hand corner of the window. Do not click on the Disconnect button or select the Disconnect option from the File menu, as this would close the connection in all windows associated with this particular connection.

6.12 New File Transfer Window

Select the New File Transfer Window option to open a File Transfer window. To make file handling as easy as possible, you can open an unlimited number of File Transfer windows.

The sequence number of each window is displayed on the window's title bar, in front of the remote host computer's name. For example, a third window associated with a connection to a host computer called remote would display as `3:remote`.

Note: To close any extra windows when you no longer need them, click on the X-shaped close button located on the window's title bar on the upper right hand corner of the window. Do not click on the Disconnect button or select the Disconnect option from the File menu, as this would close the connection in all windows associated with this particular connection.

6.13 Settings

Select the Settings option to bring up the Settings dialog. Settings can be used to control both the global settings and the profile settings for each particular remote host computer. For more information on the Settings dialog, see chapter 2 (Configuration).

6.14 Help

Select the Help option to open the SSH Secure Shell Windows client help window. In the help window you can browse, search and print help information.

6.15 Get Help On

Select the Get Help On option to change the mouse pointer to a help pointer. You can use the help pointer to click on buttons, menu items or other details of the user interface to see context sensitive help on any particular item.

6.16 File Transfer Specific Toolbar Buttons

The following toolbar buttons are available only in the File Transfer window.

Figure 6.8: The buttons that are available only in the File Transfer window are located between the Settings button and the Help button.

6.16.1 Up

Select the Up option to move the view from the current folder to its parent folder.

For example: You have a directory called `home` and it has a subdirectory called `mail`. If you are currently viewing the `mail` folder and click the Up button, the focus moves to the `home` folder.

6.16.2 Home

Select the Home option to return to your home directory on the remote host computer. This is useful if you are exploring a complex directory tree and want to quickly return to where you came from.

6.16.3 Refresh

Select the Refresh option to redraw the File Transfer window. This may be necessary if you have for example uploaded a file that does not immediately become visible on the remote host computer.

6.16.4 Download

Select the Download option to download a file - i.e. to copy it from the remote host computer to your local computer.

6.16.5 Upload

Select the Upload option to upload a file - i.e. to copy it from your local computer to the remote host computer.

6.16.6 Large Icons

Select the Large Icons option to display the file view as a Large Icons view. Each file and folder has a large icon associated with it, making for a clear and uncluttered display.

6.16.7 Small Icons

Select the Small Icons option to display the file view as a Small Icons view. Each file and folder has a small icon associated with it. This makes it possible to display several times more items than the Large Icons view.

6.16.8 List

Select the List option to display the file view as a List view. Each file and folder has a small icon associated with it, and the files and folders are displayed in one single column underneath each other.

6.16.9 Details

Select the Details option to display the file view as a Details view. The files and folders are displayed with a small icon, their file name, file size, file type, last modification date and attributes visible.

By clicking on the Name, Size, Type and Modified sort bars located on top of the File view, you can sort the files and folders based on their file name, file size, file type and the time they were last modified. Selecting the same sort option again reverses the sorting order.

Note that the sort function is not case sensitive: upper case text is sorted together with lower case text.

The file types are derived from the your local computer. If you have defined a new file type description for files with a certain file name extension, also the files in the remote computer are shown to be of that file type. This makes it easy to recognize particular file types also on the remote computer.

6.16.10 ASCII

Select the ASCII option to transfer files in ASCII mode.

6.16.11 Binary

Select the Binary option to transfer files in binary mode.

6.16.12 Auto Select

Select the Auto Select option to automatically change the transfer mode based on the file extension. Files using a file extension specified on the ASCII Extensions list on the Mode page of the Settings dialog will be transferred in ASCII mode. All other files will be transferred in binary mode. For more information, see section 2.5.17 (Mode).

6.17 Quick Connect Button

Click the Quick Connect button on the profiles toolbar to open a new connection using the default settings. For more information, see section 3.1 (Quick Connect).

6.18 Profiles Button

Click the Profiles button on the profiles toolbar to open the Profiles menu. For more information on how to use profiles, see section 3.2 (Profiles).

Chapter 7

Menu Reference

Together with the toolbar, the terminal window menus allow quick access to different terminal operations. The following menus are available: File, Edit, View, Operation (only in the File Transfer window), Window and Help.

7.1 Configuring Menus

The SSH Secure Shell menus can be configured as easily as the toolbars. You can freely select the position of the menus, and even move them into toolbars.

7.1.1 Moving Menus

You can move the SSH Secure Shell menus into new positions and arrange them so that they best serve your needs.

To move a menu, keep the `Alt` key on the keyboard pressed down and click a menu with your mouse. You will see a new mouse pointer appear. Keep the mouse button pressed down and move the menu around. When you release the mouse button, the menu will be move to a new position.

This way you can arrange the order of the menus, or even move menus into toolbars. Experiment to find the best configuration for you.

It also possible to move the individual menu options. This can be done using the Commands page of the Customize dialog (see section 2.6 (Customize)).

Note: If you move a menu to somewhere else than the menu bar or a toolbar (for example, in the terminal window text area), it is removed from the window. But don't worry - the changes become permanent only if you use the Save Settings option (see section 6.2 (Save Settings)).

7.1.2 Permanent Menu Changes

If you want to make the new menu positions permanent, use the Save Settings option (from the toolbar or the File menu) to save your settings.

If you change your mind and want to return the menus to their original positions, select the Reset Toolbars option from the View menu. A confirmation dialog will open, asking if you really want to discard the changes you have made. If you select Yes, the menus will return to their original configuration. If have modified also your toolbars, this option will reset them, too.

7.2 File Menu

The File menu allows access to the settings file and connect/disconnect operations.

7.2.1 Save Settings

Select the Save Settings option to save any changes you have made to your current settings. The default settings file where the configuration will be saved is `default.ssh2`.

If you want to save your current settings in a new settings file, select the Add Profile option under the Profiles option (see section 3.2 (Profiles)).

7.2.2 Quick Connect

Select the Quick Connect menu option from the File menu to open a new connection using the default settings. For more information, see section 3.1 (Quick Connect).

7.2.3 Profiles

Select the Profiles menu option from the File menu to open the Profiles menu. For more information on how to use profiles, see section 3.2 (Profiles).

7.2.4 Print

The Print menu option will allow you output the contents of the current scrollback buffer to a printer. For more information on printing, see section 6.3 (Print).

The Print option is available only in the terminal window.

7.2.5 Print Preview

Selecting Print Preview will display the entire contents of the scrollback buffer split into pages in the same way it will be printed. For more information on previewing the printer output, see section 6.4 (Print Preview).

The Print Preview option is available only in the terminal window.

7.2.6 Page Setup

The Page Setup menu option allows you to specify how printed pages will look. For more information, see section 2.5.20 (Printing).

The Page Setup menu option is available only in the terminal window.

7.2.7 Log Session

Choose the Log Session option to save an entire transcript of the current terminal session to a file.

When Log Session is selected, the Save As dialog opens, asking for a filename for the log file. This file will be created if it does not already exist, and it will contain a transcript of the connection. Selecting the Log Session menu item for a second time stops logging.

When logging is active, a checkmark appears next to the Log Session menu option.

The Log Session menu option is available only in the terminal window.

7.2.8 Connect

Select the Connect option to establish a new SSH connection to a remote host computer. A Connect to Remote Host dialog will appear, allowing you to specify the host name (or IP address), user name and password for the new connection.

An alternative way to establish a new connection is to press the Enter key on the keyboard when disconnected. This keyboard shortcut has the same effect as choosing the Connect option from the File menu or the toolbar.

Note that the Connect option is available only when you are not connected to any remote host computer. If you want to establish a completely new, separate SSH connection, select the Quick Connect option instead.

7.2.9 Disconnect

Select the Disconnect option to disconnect from the present remote host computer. A Confirm Disconnect dialog appears, allowing you to confirm if you really want to disconnect. Select No or Cancel to keep the

connection open, or Yes to end the connection.

Note that one connection can have several windows open (such as an SSH Secure Shell for Workstations Windows client terminal window and the File Transfer window). Disconnecting affects all windows associated with a single connection.

However, if you have started other, separate SSH Secure Shell for Workstations Windows clients, they are not affected by this disconnect operation. Disconnecting quits one connection and all of its associated windows, but none of the separate connections.

7.2.10 Exit

Select the Exit option to quit the SSH Secure Shell for Workstations Windows client. A Confirm Exit dialog appears, allowing you to confirm if you really want to exit. Select No or Cancel to keep the ssh2 client running, or Yes to exit.

Note that one connection can have several windows open (for example several File Transfer windows and several terminal windows). Exiting affects all windows associated with a single connection.

However, if you have started other, separate SSH Secure Shell for Workstations Windows clients, they are not affected by this exit operation. Exiting quits one connection and all of its associated windows, but none of the separate connections.

7.3 Edit Menu

The Edit menu allows you to copy and paste text in the terminal window and to make changes to your connection settings.

7.3.1 Copy

Select the Copy option to create a temporary copy of the selected file(s). A Download dialog is displayed, but the selected files are not yet copied to any specific location. This resembles using the Windows clipboard: You can copy files to a temporary storage and paste them later into another location.

If you do a new copy operation when the previously copied files have not yet been copied anywhere, the previous selection is lost, as the new selection replaces the old one.

Note that the copy operation is not available until you have selected one or several files or folders.

The keyboard shortcut for the copy option is `Ctrl+Insert`. The shortcut has the same effect as choosing the Copy option from the Edit menu or toolbar.

7.3.2 Paste

Select the Paste option to add previously copied files or folders into a new location. An Upload dialog is displayed when the files are pasted to the new location. This resembles using the Windows clipboard: You can copy files to a temporary storage and paste them later into another location. You can do a paste operation also by pressing `Ctrl+V` on the keyboard.

The file names of the pasted files and folders do not change during the operation. Therefore it is not possible to paste files or folders several times into one location.

Note that the paste operation is not available until you have previously copied something in the SSH Secure Shell for Workstations Windows client 'clipboard'.

The keyboard shortcut for Paste is Shift+Insert. The shortcut has the same effect as choosing the Paste option from the Edit menu or toolbar.

7.3.3 Paste Selection

Select the Paste Selection option to paste text without first copying anything to the clipboard. The Paste Selection operation copies whatever is currently selected in the terminal window to the present cursor position. If no text is selected, Paste Selection pastes the single character in the current cursor position.

This function is almost like having two different clipboards available at the same time. Paste Selection is especially useful for quick copying of text from the output of previous commands.

The Paste Selection menu item is only available in the terminal window.

7.3.4 Select All

Choose the Select All option to select all the text in the current terminal window and the scrollback buffer (or all the files and folders in the current remote directory, when using the File Transfer window).

Note that in the terminal window, the selection can span quite a few lines backwards from what is currently visible. If you want to select just what is currently displayed on screen, use the Select Screen menu option instead.

When used in the terminal window, this operation makes it fast and easy for example to save long command output strings or to create a temporary log of what is displayed on the screen.

For file transfer, this enables you to operate on the whole contents of a directory at one time. This can be especially useful when downloading, copying or deleting files.

The keyboard shortcut for Select All is Ctrl+A. This has the same effect as choosing the Select All option from the Edit menu.

7.3.5 Select Screen

Choose the Select Screen option to select all the text that is currently visible in the terminal window. Note that unlike the Select All menu option, Select Screen does not capture the scrollback buffer.

This operation can be especially useful for screen captures and quick snapshots of the command output.

The Select Screen menu option is available only in the terminal window.

7.3.6 Select None

Choose the Select None option to cancel any previous selection. This operation immediately clears the selection in the terminal window.

The Select None menu option is available only in the terminal window.

7.3.7 Find

Choosing the Find option allows you to search for text within the scrollback buffer. For more information on searching, see section 6.10 (Find).

The Find menu option is available only in the terminal window.

7.3.8 Settings

Select the Settings option to bring up the Settings dialog. Settings can be used to control both the global settings and the profile settings for each particular remote host computer. For more information on the Settings dialog, see section 2 (Configuration).

7.4 View Menu

The View menu allows you to select the way the window is displayed. The terminal window and the File Transfer window have their own set of View menu options.

7.4.1 Terminal Window View Menu Options

Toolbar

Select the Toolbar option to toggle the toolbar on and off. When the toolbar is visible, a checkmark appears next to the Toolbar menu option.

Status Bar

Select the Status Bar option to toggle the status bar on and off. When the status bar is visible, a checkmark appears next to the Status Bar menu option.

Profiles Bar

Select the Profiles Bar option to toggle the profiles bar on and off. When the toolbar is visible, a checkmark appears next to the Profiles Bar menu option.

Customize

Select the Customize option to modify the menu options, toolbars, menu settings and general settings. The Customize dialog opens. For more information on customizing the user interface, see section 2.6 (Customize).

Reset Toolbars

Select the Reset Toolbars option to reset the toolbar and menu positions to their original state. This is a good choice if you regret the changes you have made, or have misplaced some menu or toolbar option.

Reset Terminal

Select the Reset Terminal option to reset the terminal settings to the state they were in when connecting. This will clear the terminal window and the scrollback buffer and reset the keymap, characterset and fonts.

7.4.2 File Transfer View Menu Options

Toolbar

Select the Toolbar option to toggle the toolbar on and off. When the toolbar is visible, a checkmark appears next to the Toolbar menu option.

Status Bar

Select the Status Bar option to toggle the status bar on and off. When the status bar is visible, a checkmark appears next to the Status Bar menu option.

Profiles Bar

Select the Profiles Bar option to toggle the profiles bar on and off. When the toolbar is visible, a checkmark appears next to the Profiles Bar menu option.

Customize

Select the Customize option to modify the menu options, toolbars, menu settings and general settings. The Customize dialog opens. For more information on customizing the user interface, see section 2.6 (Customize).

Reset Toolbars

Select the Reset Toolbars option to reset the toolbar and menu positions to their original state. This is a good choice if you regret the changes you have made, or have misplaced some menu or toolbar option.

Large Icons

Select the Large Icons option to display the file view as a Large Icons view. Each file and folder has a large icon associated with it, resulting in a clear and uncluttered display.

If the Large Icons option is selected, a selection marker appears next to the Large Icons menu option.

Small Icons

Select the Small Icons option to display the file view as a Small Icons view. Each file and folder has a small icon associated with it. This makes it possible to display several times more items than the Large Icons view.

If the Small Icons option is selected, a selection marker appears next to the Small Icons menu option.

List

Select the List option to display the file view as a List view. Each file and folder has a small icon associated with it, and the files and folders are displayed in one single column underneath each other.

If the List option is selected, a selection marker appears next to the List menu option.

Details

Select the Details option to display the file view as a Details view. The files and folders are displayed with a small icon, their file name, file size, file type, last modification date and attributes visible.

By clicking on the Name, Size, Type and Modified sort bars located on top of the File view, you can sort the files and folders based on their file name, file size, file type and the time they were last modified. Selecting the same sort option again reverses the sorting order.

Note that the sort function is not case sensitive: upper case text is sorted together with lower case text.

The file types are derived from the your local computer. If you have defined a new file type description for files with a certain file name extension, also the files in the remote computer are shown to be of that file type. This makes it easy to recognize particular file types also on the host computer.

Arrange Icons

Select the Arrange Icons option to open a submenu where you can select in which order the files and folders are displayed in the file view. A selection marker appears next to the currently selected Arrange Icons option.

By Name: The files and folders are arranged alphabetically based on their file name.

By Type: The files and folders are arranged alphabetically based on their file type.

By Size: The files are arranged by their file size. Folders are arranged alphabetically.

By Date: The files and folders are arranged by the time they were last modified.

If you have selected the Details view, you can achieve the same effect by clicking on the Name, Size, Type and Modified sort bars located on top of the File view. Selecting the same Arrange Icons option again reverses the sorting order.

Note that the sort function is not case sensitive: upper case text is sorted together with lower case text.

Show Root Directory

Select the Show Root Directory option to toggle if the root directory is displayed in the folder view. If the root directory is not displayed, you are not able to select or view any folders above your home directory in the directory tree hierarchy. By default the root directory is not displayed.

If the Show Root Directory option is selected, a selection marker appears next to the Show Root Directory menu option.

Show Hidden Files

Select the Show Hidden Files option to toggle if the normally hidden files in the remote host computer are displayed in the file view.

By default, UNIX hosts do not display any files or directories that begin with the dot (.) character, such as .rhosts or .profile. Selecting the Show Hidden Files option corresponds to specifying the `-a` switch of the ls command.

If the Show Hidden Files option is selected, a selection marker appears next to the Show Hidden Files menu option.

Refresh

Select the Refresh option to redraw the File Transfer window. This may be necessary if you have for example uploaded a file that does not immediately become visible on the remote host computer.

The keyboard shortcut for Refresh is `F5`.

7.5 Operation Menu

The Operation menu allows you to copy files to and from the remote host computer, and to navigate the remote directory structure. The Operation menu is available only in the File Transfer window.

7.5.1 Open

The Open option can be used to view a file on the remote host computer. First select a file from the File Transfer window and the select the Open option. The file will be downloaded and displayed.

7.5.2 Upload

Select the Upload option to upload a file - i.e. to copy it from your local computer to the remote host computer.

The keyboard shortcut for Upload is `Ctrl+U`. This has the same effect as choosing the Up option from the Operation menu or the toolbar.

7.5.3 Download

Select the Download option to download a file - i.e. to copy it from the remote host computer to your local computer.

Note that you must first select the remote file(s) before selecting Download. If no files or folders are selected, the Download menu option is grayed out.

The keyboard shortcut for Download is Ctrl+D. This has the same effect as choosing the Download option from the Operation menu or the toolbar.

7.5.4 Up

Select the Up option to move the view from the current folder to its parent folder.

For example: You have a directory called `home` and it has a subdirectory called `mail`. If you are currently viewing the `mail` folder and click the Up button, the focus moves to the `home` folder.

The keyboard shortcut for Up is the Backspace key. This has the same effect as choosing the Upload option from the Operation menu or the toolbar.

7.5.5 Home

Select the Home option to return to your home directory on the remote host computer. This is useful if you are exploring a complex directory tree and want to quickly return to where you came from.

The keyboard shortcut for Home is Ctrl+H. This has the same effect as choosing the Home option from the Operation menu or the toolbar.

7.5.6 Go To Folder

Select the Go to Folder option to enter a folder where you want to move directly. A Go to Folder dialog appears, allowing you to type in the path to the desired directory. The current directory path is displayed in the text field for your reference, eliminating the need to type in long directory paths from scratch. Type in the desired directory path and press `Enter`. The specified directory instantly appears.

If you specify a directory that does not exist, the file view turns blank and the nonexistent directory appears in the folder view as a red folder, meaning that such a folder is not accessible to you. These 'false directories' can serve as useful reminders that you have tried to access directories with such names, but remember that they may not actually exist on the remote host computer.

The keyboard shortcut for Go To Folder is Ctrl+G. This has the same effect as choosing the Go to Folder option from the Operation menu.

7.5.7 New Folder

Select the New Folder option to create a new folder on the remote host computer. A new folder appears on file view along with a text field where you can type in the name for the new folder.

If you do not type a name for the new folder but just hit `Enter`, a new folder is not created.

The keyboard shortcut for New Folder is Ctrl+N. This has the same effect as choosing the New Folder option from the Operation menu.

7.5.8 Delete

Select the Delete option to delete file(s) or folder(s) on the remote host computer. A Confirm Delete dialog appears, allowing you to confirm if you really want to delete the selected files or folders. Select No or Cancel to keep the selected items, or Yes to delete them.

The keyboard shortcut for Delete is the Delete key. This has the same effect as choosing the Delete option from the Operation menu.

7.5.9 Rename

Select first a file from the File Transfer window and then the Rename option to rename the file.

The keyboard shortcut for rename is F2. This has the same effect as choosing the Rename option from the Operation menu.

You can also rename a file by clicking on the file with the right mouse button. A shortcut menu containing the Rename option will appear.

Please note that the rename operation requires an SSH Secure Shell server version 2.2.0 (or later). Earlier SSH Secure Shell server versions do not support the rename operation, and using this option will produce the Error Renaming File message - for more information, see section 9.2.10 (Error Renaming).

7.5.10 Properties

Select first a file from the File Transfer window and then the Properties option to view the file properties.

You can also view a file's properties by clicking on the file with the right mouse button. A shortcut menu containing the Properties option will appear. You can select multiple files and view their properties.

For more details about the Properties Page, see section 5.10 (File Properties).

7.5.11 File Transfer Mode

Select the File Transfer Mode option to set in which transfer mode files will be transferred. A submenu opens, containing the following options:

ASCII

Select ASCII option to transfer files in ASCII mode.

Binary

Select the Binary option to transfer files in binary mode.

Auto Select

Select the Auto Select option to automatically change the transfer mode based on the file extension. Files using a file extension specified on the ASCII Extensions list on the Mode page of the Settings dialog will be transferred in ASCII mode. All other files will be transferred in binary mode. For more information, see section 2.5.17 (Mode).

7.6 Window Menu

The Window menu allows you to open and close different types of windows.

7.6.1 New Terminal

Select the New Terminal option to open a new SSH Secure Shell for Workstations Windows client terminal window. The new window is immediately connected to the same remote host computer as the current window, saving you the trouble of typing your password again.

Multiple windows to a single connection allow you to for example debug your code in one window, execute it in another, display reference information in a third one and read your mail in a fourth window.

The sequence number of each window is displayed on the window's title bar, in front of the remote host computer's name. For example, a second window associated with a connection to a host computer called remote would display as `2:remote`.

To close any extra windows when you no longer need them, click on the X-shaped close window button located on the window's title bar on the upper right hand corner of the window. Do not click on the Disconnect

button or select the Disconnect option from the File menu, as this would close the connection in all windows associated with this particular connection.

7.6.2 New File Transfer

Select the New File Transfer option to open a new File Transfer window. To make file managing as easy as possible, you can open an unlimited number of File Transfer windows.

The sequence number of each window is displayed on the window's title bar, in front of the remote host computer's name. For example, a third window associated with a connection to a host computer called remote would display as `3:remote`.

To close any extra windows when you no longer need them, click on the X-shaped close window button located on the window's title bar on the upper right hand corner of the window. Do not click on the Disconnect button or select the Disconnect option from the File menu, as this would close the connection in all windows associated with this particular connection.

7.6.3 New Explorer

Select the New Explorer option to open a new Windows Explorer window. The Windows Explorer is the familiar Windows utility that can be used to manage the files and folders in your local computer. You can have multiple Explorer windows open at the same time to make file management easier.

The New Explorer menu option is available only in the File Transfer window.

7.6.4 Close

Select the Close option to close the current window. Other windows are unaffected, even if they are associated with the same connection.

7.6.5 Close All Others

Select the Close all Others option to close all the other SSH Secure Shell for Workstations Windows client windows associated with this particular connection.

A single connection can have several windows open (such as an SSH Secure Shell for Workstations Windows client terminal window and a File Transfer window). The Close All Others operation affects all the other windows associated with a particular connection.

However, if you have started other, separate SSH Secure Shell for Workstations Windows clients, they are not affected by this operation. Close All Others only affects one connection and all of its associated windows, but no other, separate connections.

7.7 Help Menu

The Help menu allows you to access the help and copyright information.

7.7.1 Contents

Select the Contents option from the Help menu to view the help as Web pages. A browser will open and the HTML based help files will be loaded locally, from your own computer. The contents page will appear. Click on a chapter you want to explore, or click the Index link to see an alphabetical listing of keywords.

If you want to check the Web help instead of the locally installed help files, see the SSH Secure Shell for Workstations Windows client Web help: `http://www.ssh.com/products/ssh/winhelp/`.

7.7.2 Get Help On

Select the Get Help On option to change the mouse pointer to a help pointer. You can use the help pointer to click on buttons, menu items or other details of the user interface to see context sensitive help on any particular item.

7.7.3 SSH on the Web

Select the SSH on the Web option to open a submenu containing Web links to SSH Secure Shell Web pages.

Online Help

Select the Online Help option to load the Web version of the SSH Secure Shell for Workstations Windows client help (`http://www.ssh.com/products/ssh/winhelp/`). This is useful if you want to see the most up-to-date version of the help.

Frequently Asked Questions

Select the Frequently Asked Questions option to load the online version of the SSH Secure Shell for Workstations Windows client FAQ (`http://www.ssh.com/faq/`).

Home Page

Select the Home Page option to open the SSH Communications Security home page (`http://www.ssh.com`).

7.7.4 Troubleshooting

Select the Troubleshooting option to display the Troubleshooting dialog. If you encounter problems when using the SSH Secure Shell for Workstations Windows client, you can send a bug report by using the support web form at `http://www.ssh.com/support`. To make the support team's work easier, you should describe your system and the problem situation as carefully as possible. The Troubleshooting dialog helps you in this.

Click the Copy to Clipboard button to copy the troubleshooting report on the Windows clipboard. You can then paste (`Ctrl+V`) the report into the support web form. But please describe your problem also in your own words - the Troubleshooting dialog cannot do that for you!

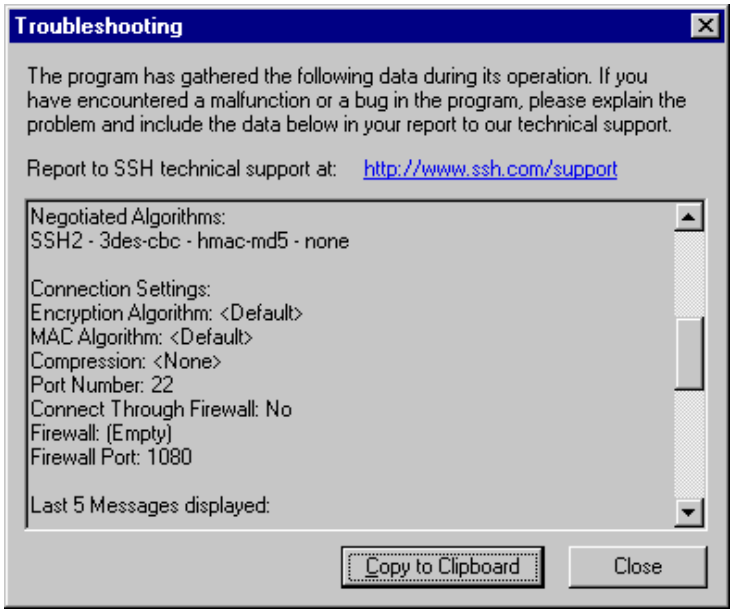

Figure 7.1: The Troubleshooting dialog.

7.7.5 Debugging

Select the Debugging option to gather debugging information useful for tracking possible errors. The Debugging dialog opens.

Enable Debugging

Select the **Enable Debugging** check box to log debugging information. Enabling this option slows down the client, so it should be only done to track error situations, for example when requested by SSH technical support.

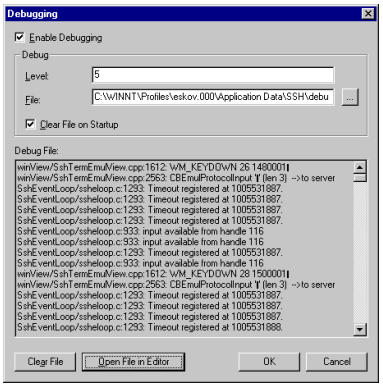

Figure 7.2: The Debugging dialog

Debug

The **Debug** options define how much debugging information will be collected and where the data will be saved.

Level

Type in a number to indicate the debug level. Higher numbers will produce more debugging data. A typical value for debug level is 3 or 4. Debug levels approaching 10 will produce large amounts of debugging data and make the software very slow.

Alternatively you can specify different debug levels for different operations. For example the debug value `4, sshevent loop=7` would define the general debug level as 4, but for `sshevent loop` activity the debug level would be 7.

File

Select the file where debug data will be saved. Either type in the path and filename, or click the button on the righthand side of the text field to open a **Save As** dialog, allowing you to locate the save file.

Clear File on Startup

Select the **Clear File on Startup** check box to delete the debug data every time SSH Secure Shell is launched.

Note: If this option is not checked, the log file will keep continuosly growing and must be manually manually cleared.

Debug File

The **Debug File** displays a scrollable view of the currently gathered debug data.

Clear File

Click the **Clear File** button to empty the current debug data file.

Open File in Editor

Click the **Open File in Editor** button to open the current debug data file in a text editor, allowing you to view, edit, save or print the data.

OK

Click the **OK** button to accept the current settings and close the Debugging dialog.

Cancel

Click the **Cancel** button to discard the changes and close the Debugging dialog.

7.7.6 Import License File

With the Import License File option you can register your copy of the SSH Secure Shell for Workstations Windows client.

After you have applied for a license file from the SSH e-commerce web site (`http://commerce.ssh.com`) and received a license file (which is called `license.dat` by default), select the Import License File menu option from the Help menu. You will be presented with a dialog requesting a file name. Locate the `license.dat` file and click the OK button. You should see a dialog telling that the license file was successfully imported and copied to the installation directory. Click the OK button to continue. Your copy of the SSH Secure Shell for Workstations Windows client is now registered.

7.7.7 About Secure Shell

Select the About Secure Shell option to view the copyright information on the SSH Communications Security's SSH Secure Shell for Workstations Windows client. Also version and license information is displayed. Click the OK button to close the dialog.

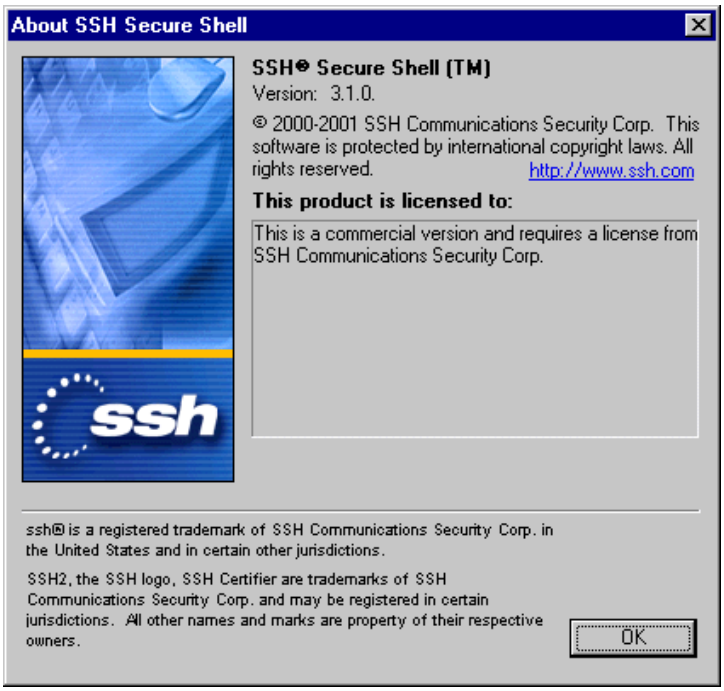

Figure 7.3: The About dialog displays copyright, licensing and version information.

Chapter 8

Advanced Information

SSH is a protocol for secure remote login and other secure network services over an insecure network. It consists of three major components:

- Transport layer protocol [SSH-TRANS] provides server authentication, confidentiality, and integrity. It may optionally also provide compression. The transport layer will typically be run over a TCP/IP connection, but might also be used on top of any other reliable data stream.
- User authentication protocol [SSH-USERAUTH] authenticates the client-side user to the server. It runs over the transport layer protocol.
- Connection protocol [SSH-CONN] multiplexes several logical channels into the encrypted tunnel. It runs over the user authentication protocol.

The client sends a service request once a secure transport layer connection has been established. A second service request is sent after user authentication is complete. This allows new protocols to be defined and coexist with the protocols listed above.

The connection protocol provides channels that can be used for a wide range of purposes. Standard methods are provided for setting up secure interactive shell sessions and for forwarding (”tunneling”) arbitrary TCP/IP ports and X11 connections.

8.1 SSH2 Functionality

The SSH Secure Shell for Workstations Windows client connects and logs into the specified remote host computer. Upon login, the user must prove his identity to the remote host computer by using some authentication method.

Public-key authentication is based on the use of digital signatures. Each user creates a public / private key pair for authentication purposes. The server knows the user's public key, but only the user has her private key.

When the user tries to authenticate herself, the server sends a challenge to the user. User is authenticated by signing the challenge using the private key.

Private / public key pairs can be created with a built-in key generation wizard. (See section 3.3.1 (Key Generation Wizard).)

Other authentication methods can be used as well. If other methods fail, the SSH Secure Shell for Workstations Windows client prompts for a password. Since all communications is encrypted, the password will not be available for eavesdroppers.

When the user's identity has been accepted by the server, the server either executes the given command, or logs into the remote host computer and gives the user a normal shell on the remote computer. All communication with the remote command or shell will be automatically encrypted. The session can be transparent and can be used to reliably transfer binary data.

The session terminates when the command or shell on the remote machine exits and all X11 and TCP/IP connections have been closed. The exit status of the remote program is returned as the exit status of ssh2.

If the user is using X11, the connection to the X11 display is automatically forwarded to the remote side in such a way that any X11 programs started from the shell (or command) will go through the encrypted channel, and the connection to the real X server will be made from the local machine.

SSH2 will also automatically set up Xauthority data on the server machine. For this purpose, it will generate a random authorization cookie, store it in Xauthority on the server, and verify that any forwarded connections carry this cookie and replace it by the real cookie when the connection is opened. The real authentication cookie is never sent to the server machine (and no cookies are sent in the plain).

If the user is using an authentication agent, the connection to the agent is automatically forwarded to the remote side unless disabled.

Forwarding of arbitrary TCP/IP connections over the secure channel can be specified. TCP/IP forwarding can be used for secure connections to electronic wallets or going through firewalls.

SSH2 automatically maintains and checks a database containing public keys of hosts. When logging on to a host for the first time, the host's public key is stored to a file in the user's personal directory. If a host's identification changes, SSH2 issues a warning and disables password authentication to prevent for example a malicious Trojan horse program from getting the user's password. Another purpose of this mechanism is to prevent man-in-the-middle attacks that could otherwise be used to circumvent the encryption.

SSH2 also has built-in support for SOCKS version 4 for traversing firewalls.

8.1.1 Host Keys

Each server host must have a host key. Hosts may have multiple host keys using multiple different algorithms. Multiple hosts may share the same host key. Every host must have at least one key using each required public key algorithm.

The server host key is used during key exchange to verify that the client is really communicating with the correct server. For this to be possible, the client must have prior knowledge of the server's public host key.

Two different trust models can be used:

- The client has a local database that associates each host name (as typed by the user) with the corresponding public host key. This method requires no centrally administered infrastructure, and no third-party coordination. The downside is that the database of name-key associations may become burdensome to maintain.
- The host name - key association is certified by a trusted certification authority. The client knows only the CA root key, and can verify the validity of all host keys certified by accepted CAs.

  The second alternative eases the maintenance problem, since ideally only a single CA key needs to be securely stored on the client. On the other hand, each host key must be appropriately certified by a central authority before authorization is possible. Also, a lot of trust is placed on the central infrastructure.

8.1.2 Security Properties

The primary goal of the SSH protocols is improved security on the Internet.

- All encryption, integrity, and public key algorithms used are well-known, well-established algorithms.
- All algorithms are used with cryptographically sound key sizes that are believed to provide protection against even the strongest cryptanalytic attacks for decades.
- All algorithms are negotiated, and in case some algorithm is broken, it is easy to switch to some other algorithm without modifying the base protocol.

8.2 Public-Key Infrastructure (PKI)

A system that uses digital certificates for authentication and thus helps establish secure communications is called a public-key infrastructure (PKI). A PKI consists of end entities, certification authorities (trusted parties who sign and issue certificates), and registration authorities (parties who handle the identification of end entities).

(Please note that PKI and PKCS #11 support is only available in commercial distributions of the SSH Secure Shell for Workstations client.)

A PKI provides a means for reliable authentication of parties in an online environment by using asymmetric encryption. In addition to authentication, the PKI also enables secure digital communications and transactions.

In asymmetric encryption, every entity (communicating party) has a key pair that consists of a public key and a private key. Private keys are secret and are known only to their owners. Private keys are used for signing and decrypting messages.

Public keys are, as the name implies, public and can be published on, for example, a web server. Public keys are used for validating signatures and encrypting messages. Before public-key operations can be made, the public key has to be received securely so that no one can substitute the genuine key with a tampered one. Certificates can be used for distributing public keys of end entities.

Certificates are digital documents that are used for secure authentication of communicating parties. Certificates are also used for sending the public keys of the entities to other entities. A certificate binds identity information about an entity to the entity's public key for a certain validity period. Certificates can be thought of as analogous to passports that guarantee the identity of their bearers.

To enable wide usage of certificates and interoperable implementations from multiple vendors, certificates have to be based on standards. The most advanced and widespread certificate specifications at the moment are defined by the PKIX Working Group of the IETF (Internet Engineering Task Force).

8.2.1 CA

The trusted parties that sign, issue and manage certificates are called certification authorities (CA). A CA is the instance that vouches for the identity and trustworthiness of the end entity it grants the certificates to. Certification authorities can be thought of as being analogous to governments issuing passports for their citizens.

CA can be a third party trusted by everyone in the PKI, or it can belong to the same organization as the end entities. CAs can also certify other CAs (to issue certificates) by signing so-called CA certificates. This leads to a tree-like structure of CA hierarchies. The top CA in the "tree" is called a root CA. A new root CA is established in two steps:

1. Generation of a CA key pair and a CA certificate.

2. Exporting the CA public key "out-of-band" to all end entities in the PKI.

The public keys of CAs are usually built into specific client applications. CA keys are then distributed when the client applications are installed to the end users' devices (workstations, laptops, PDAs). Before end entities can communicate securely, also their public keys need to be certified by enrolling the end entities into the PKI and having their certificates issued by the CA.

8.2.2 Certificate Enrollment

Certificate enrollment is an action in which a CA certifies a public key. A certification authority can delegate authentication of the end entities as well as certain other administrational tasks to so-called registration authorities (RA). Using local RAs a large geographically or operationally distributed PKI can work in a scalable way, even when the actual certificate issuing is centralized.

The actual enrollment process consists of the following steps:

1. Generation of a key pair
2. End entity requesting certification for the public key
3. CA or RA verifying the identity of the end entity
4. CA generating a certificate for the end entity and making it available (if the request is approved).

End entities can use standard request formats to request certificates from a CA. The CA uses the underlying policy to decide whether to approve the request or not. The policy decision and the approval/denial can be automatic, or it may be required that the operator of the CA has to approve certificate requests manually. If identification of the end entity is needed, the RA may perform this function. If the request is approved, a signed certificate will be issued and delivered to a public directory. Finally, when the issued certificates are available in the directories, all entities in the PKI can verify each other's certificates with the CA's public key.

8.2.3 Certificate Revocation

If a private key of an end entity is compromised or the right to authenticate with a certificate is lost during the certificate's validity period, the certificate has to be revoked, and all PKI users have to be informed about this. Certificate revocation lists (CRL) can be used for this purpose.

A CRL is a time-stamped list identifying the revoked certificates and is signed by a CA. The presence of the signature allows CRLs to be distributed via un-trusted channels in public directories, just like the certificates. Each CA issues CRLs on a regular basis, the issuance period being defined in the CA's security policy. Certificate validation has to include the retrieval of the latest CRL to check the status of the certificate. X.509 v2 CRL is a standard PKIX CRL format.

As the certificate revocation lists are updated on a periodic basis, they don't provide real-time status information for the PKI. If more strict security needs to be followed, online status data has to be provided for relying end entities. In Online Certificate Status Protocol (OCSP) OCSP responders respond to end entities' status requests with signed responses about the revocation status of a certificate. This kind of function is required for example in a PKI where high-value business transactions are digitally signed.

8.2.4 Directory Services

Certificates and CRLs have to be distributed to directories in order to be available to PKI users. Information about how CRLs are to be obtained can be indicated in an extension field (distribution point) of an X.509 v3 certificate.

The Lightweight Directory Access Protocol (LDAP) has become a de facto standard procedure for CRL and certificate distribution. This enables interoperability with third party directory servers based on the LDAP standard. OCSP can be seen as an replacement for LDAP since with it revocation lists are not needed. However, encryption certificates still need to be fetched from somewhere, such as an LDAP directory.

8.3 Using Certificate Authentication

In order to use certificate authentication you need to issue certificates for users and hosts using a certification authority (CA) software such as SSH Certifier(TM).

The first requirement for using certificates is to import the certificates of the CAs that you trust. Trusting a CA means that to the best of your knowledge the private key of the CA has not been compromised. The CA certificates will be the connecting links between entities that have been issued a certificate.

Requesting a CA to issue a certificate is called *certificate enrollment*. SSH Secure Shell supports the CMPv2 enrollment protocol. If CMPv2 is not available in the CA software, the enrollment can be done in another application and the resulting certificates can be imported to SSH Secure Shell using the PKCS #12 format.

PKCS #12 format files can contain one or more user or CA certificates and private keys. SSH Secure Shell determines the contents of the file and writes the entries to the corresponding directories for subsequent use. Standard PKCS #12 files generated using applications such as Netscape Navigator and Microsoft Internet Explorer are supported.

Other supported formats for importing user and CA certificates are PKCS #7, BER and X.509 binary. If a user certificate is imported the corresponding private key must be made available to SSH Secure Shell. For this purpose, PKCS #12 is recommended.

In the certification request you can suggest a Common Name (e.g. *John Smith*), Organization Unit (like *Marketing*), Organization (*SSH Communications Security Corp.*), Country (*US*) and Email Address (*john.smith@ssh.com*).

The CA can change these fields before issuing the certificate. The certificate validity period and other parameters are determined by the configuration of the CA software. Please note that certificate enrollment requiring manual acceptance in the CA software is not supported. You may be able to compensate this by using PKCS #12 file importing.

8.3.1 PKCS #11

PKCS #11 is a runtime interface to hardware tokens and software keys. To be able to use a hardware token, such as a smart card or a USB token, a third party driver is required. The driver is usually a single DLL (Dynamic Link Library) file residing in the Windows system directory. You need to install the software included with the hardware token before configuring SSH Secure Shell.

Chapter 9

Troubleshooting

If you should encounter an error message when using the SSH Secure Shell for Workstations Windows client, please read the error message carefully and follow the suggested course of action. Some possible error messages and their suggested corrective actions are described below.

9.1 Error Dialogs At Startup

If you get an error dialog when you try to run SSH Secure Shell, you may need to update the common controls library, `comctl32.dll`. The older library version is included in at least some Windows 95 installations. To obtain the update, go to the Microsoft web site `http://www.microsoft.com/msdownload/ieplatform/ie/comctrl x86.asp` and download the latest version.

9.1.1 Evaluation Period Ending

This message indicates that the evaluation period for this copy of SSH Secure Shell client will soon end. You are allowed to use the client for free for the duration of the evaluation period, and after that you should obtain a license in order to continue using the software.

For more information on the license agreement, read the file license.txt located in the directory where SSH Secure Shell for Workstations Windows client was installed.

Now is a good time to register the software to ensure that your network connections will always be secure. The fastest and most convenient way to obtain a license for your SSH Secure Shell client is to visit the SSH e-commerce web site at `http://commerce.ssh.com/`.

The licensing is a quick and easy operation. The license file is a small, fast loading file that you can download immediately. You can import the license file (license.dat) by selecting the Import License File option from the Help menu.

You will be presented with a dialog requesting a file name. Locate the license.dat file and click the OK button. You should see a dialog telling that the license file was successfully imported. Click the OK button to continue. Your copy of the SSH Secure Shell for Workstations is now registered.

Alternatively, if you want to download the newest version of the licensed SSH Secure Shell Windows Client software, you can download the whole package with the license already installed.

Thank you for evaluating the SSH Secure Shell Windows Client!

9.1.2 Expiration

This error indicates that the evaluation period for this copy of the SSH Secure Shell client has ended. The client software cannot be used until you obtain a valid license.

For more information on the license agreement, read the file license.txt located in the same directory as the SSH Secure Shell Windows Client.

The fastest and most convenient way to obtain a license for your SSH Secure Shell client is to visit the SSH e-commerce web site at `http://commerce.ssh.com/`.

The licensing is a quick and easy operation. The license file is a small, fast loading file that you can download immediately. You can import the license file (license.dat) by selecting the Import License File option from the Help menu.

You will be presented with a dialog requesting a file name. Locate the license.dat file and click the OK button. You should see a dialog telling that the license file was successfully imported. Click the OK button to continue. Your copy of the SSH Secure Shell for Workstations is now registered.

Alternatively, if you want to download the newest version of the licensed SSH Secure Shell Windows Client software, you can download the whole package with the license already installed.

Thank you for evaluating the SSH Secure Shell for Workstations!

9.1.3 Failed To Read Keymap File

This error message indicates that for some reason the SSH Secure Shell for Workstations Windows client is unable to read the KEYMAP.MAP file. When the ssh2 client is started for the first time, it checks for the existence of the keymap file, and if the client does not find it, it copies it to the current user's personal directory.

For easy access to your personal data files, open the Profile Settings page of the Settings dialog and click the Browse button.

Check that the KEYMAP.MAP file is in the correct folder and that its Read-only attribute is not set.

9.1.4 File Open Error

This error indicates that a configuration file (such as KEYMAP.MAP or default.ssh2) could not be properly opened. The file may be damaged, or the file may define an unknown configuration value.

This error may indicate that you are using a configuration file that was created using an earlier version of the SSH Secure Shell client. You can remedy this by saving your configuration file again (select the Save option from the File menu).

9.1.5 Keymap Error

This error indicates that the SSH Secure Shell client has not been able to read a keymap file (`KEYMAP.MAP`, `KEYMAP22.MAP` or `OUTPUT.MAP`) that defines how the keyboard input/output is processed. The keymap file is either missing, corrupted or renamed with an unrecognizable file name.

Close the SSH Secure Shell client and check the keymap file. If it is missing or corrupted, reinstall the SSH Secure Shell client. The new installation will leave your saved configuration settings intact, and after reinstalling you can continue using SSH Secure Shell client as before.

9.1.6 Your License Has Expired

This error indicates that the license for this copy of the SSH Secure Shell for Workstations Windows client has expired. The client software cannot be used until you obtain a new license.

For more information on the license agreement, read the file license.txt located in the same directory as the SSH Secure Shell Windows Client.

The fastest and most convenient way to obtain a license for your SSH Secure Shell client is to visit the SSH e-commerce web site at `http://commerce.ssh.com/`.

The licensing is a quick and easy operation. The license file is a small, fast loading file that you can download immediately. You can import the license file (license.dat) by selecting the Import License File option from the Help menu.

You will be presented with a dialog requesting a file name. Locate the license.dat file and click the OK button. You should see a dialog telling that the license file was successfully imported. Click the OK button to continue. Your copy of the SSH Secure Shell for Workstations is now registered.

Alternatively, if you want to download the newest version of the licensed SSH Secure Shell for Workstations software, you can download the whole package with the license already installed.

Thank you for using the SSH Secure Shell for Workstations Windows client!

9.2 Error Dialogs During Operation

The following error dialogs may occur when operating SSH Secure Shell.

9.2.1 Authentication Failure

This error message indicates that the authentication process between your local computer and the remote host computer has for some reason failed.

The most common cause for failed authentication is an incorrect password, likely caused by a typing mistake.

Also the user name may be incorrect. Check that you have typed it correctly.

One possible reason for authentication failure is that the remote host computer may have been configured to require several authentication methods to be used. For example both password and public key authentication could be used for increased security. Even if you entered your password correctly, some other required authentication method could have failed. A relatively common situation is one where the remote host computer is expecting public-key authentication and you have not sent your public key to the host. You can do this by following the instructions in section 3.5 (Uploading Your Public Key).

It may also be possible that your account on the remote host computer has been disabled or that the remote host computer is having temporary problems causing errors with the login procedure.

Try to connect again and carefully type in your user name and password. If after a couple of retries you are sure that you have entered both of them correctly, contact the system administrator of the remote host computer.

9.2.2 Confirm Disconnect

This dialog is displayed when you are disconnecting an active connection. You can either confirm the disconnect operation or cancel it.

Yes

Click the Yes button to close the currently active connection.

No

Click the No button to keep the current connection.

Cancel

Click the Cancel button to change your mind and abort the disconnect operation. This has the same effect as selecting No. (This option is included to make the selection more intuitive for users who have clicked the Disconnect button in error.)

Help

Click the Help button to view the help.

Note that one connection can have several windows open (such as an SSH Secure Shell for Workstations Windows client terminal window and a File Transfer window). Disconnecting affects all windows associated with a single connection. All tunnels associated with the disconnected connection will be terminated as well.

However, if you have started other, separate SSH Secure Shell for Workstations Windows clients, they are not affected by this disconnect operation. Disconnecting quits one connection and all of its associated windows, but no other, separate connections. You can differentiate between different windows associated with a single connection by the window's sequence number, displayed on the title bar.

You can differentiate between different windows associated with a single connection by the window's sequence number, displayed on the title bar (see section 4.1 (Terminal Window Title Bar)).

9.2.3 Confirm File Overwrite

The Confirm File Overwrite dialog indicates that a file you are transfering already exists in the target system. You can choose if you want to replace the old file with the transferred file.

You have the following options:

Yes

Click the Yes button to replace the old file.

Yes to All

Click the Yes to All button to replace this file and also all the other files that already exist in the target system.

No

Click the No button to avoid overwriting the already existing file.

Cancel

Click the Cancel button to abort the file transfer operation.

9.2.4 Connection Failure

This error indicates that the SSH Secure Shell client cannot establish a connection to the remote host computer. There are several reasons that might cause this situation.

It may be that you have simply made a typing mistake, and there is an error in the name of the remote host computer. In this case you should also receive an error stating that the host is unknown.

Check that you have defined the correct port number for the connection. The port can be changed on the Connection page of the Settings dialog.

There may be problems with the configuration or physical setup of the network connection. Verify that other network connections are functioning.

This problem may also arise if your local system is protected by a firewall and the firewall has not been properly configured. If you suspect that this is the case, ask your local system administrator to reconfigure the firewall.

There may also be a temporary problem with the remote host computer. If this is the case, you should wait for a while and try to connect again later. Contact the administrator of the remote host computer for additional information.

9.2.5 Disconnected; Authentication Error

The error message "Disconnected; Authentication Error (No further authentication methods available.)" indicates that any of the methods that have been used to authenticate you to the server have not been successful.

A relatively common situation is one where the remote host computer is expecting public-key authentication to be used and you have not sent your public key to the host. You can do this by following the instructions in section 3.5 (Uploading Your Public Key).

This error is also produced if the system's name server is not doing reverse lookups correctly. Ask your system administrator to configure the name server so that it does reverse lookups properly.

If this is not possible, the system administrator has to edit the file `/etc/ssh2/sshd2_config` on the SSH server and change the `RequireReverseMapping` setting to `no`.

This is a common problem for modem connections. Typical modem connections use dynamic IP addresses. This means that the IP address changes from one connection to another, and these dynamic IP addresses have no permanent name server entries in the Domain Name System (DNS). If this is the case, you will have to ask your service provider to edit the sshd2_config file on the SSH server.

9.2.6 Disconnection

This error indicates that the connection to the remote host computer has been lost.

There may be problems with the configuration or the physical setup of either your or the remote host computer's network connection.

It may also be that the remote host computer has been rebooted, which has disconnected your computer from the host.

Usually problems of this kind are temporary, and you can try again after waiting for a while. If this does not

help, check your local network, and if necessary, contact also the system administrator of the remote host computer.

9.2.7 Enter Passcode

When using SecurID for authentication, you have to enter the passcode in order to authenticate the connection. In some situations you may not be able to do this immediately, but will have to wait for the token to change.

9.2.8 Enter Passphrase For Private Key

This message indicates that the remote host computer is willing to accept your public key to authenticate you in the future.

Type in the passphrase associated with this key. (You defined the passphrase when you created the public key - see section 3.3.5 (Key Generation - Enter Passphrase) for more information.)

If you just press the Enter key, public authentication will not be used, and the system will ask you to type in your password instead.

9.2.9 Enter PIN

When using certificate authentication, the Enter PIN dialog will display information on the provider used. You will have to enter the personal identification number (PIN) associated with the token.

9.2.10 Error Renaming

This error message indicates that a file or folder on the remote host computer could not be renamed. Usually this means that the SSH server software is too old to support renaming.

The rename operation requires an SSH Secure Shell server version 2.2.0 (or later). Earlier SSH Secure Shell server versions do not support the rename operation. Renaming remote files or folders is not possible until the system administrator of the remote host computer updates the SSH server software.

9.2.11 Failed To Create An Incoming Tunnel

This error indicates that the system has not been able to create the requested tunnel.

The most common reason for this failure is that a tunnel with the same name already exists. The similarly named tunnel may have been created by another SSH Secure Shell client connected to the same server.

If the system has several of Secure Shell users, they may already have reserved several available ports. In this case just try again to find a free port.

Another possible reason is that you have no permission to open the requested port. The system administrator may have set a policy that restricts opening of communications ports - this is common practice especially with incoming ports. Check the local policy from the system administrator. Please note that only the system administrator (root) can open port numbers under 1024.

Please note that both incoming and outgoing tunnels produce their own error messages. If both fail, the client will display two separate error messages.

9.2.12 Host Identification

When you connect to a remote host computer for the first time, the host sends your local computer its public key in order to identify itself. To help you to verify the host's identity, the Host Identification dialog displays a fingerprint of the host's public key. The fingerprint is represented using the SSH Babble format, and it consists of a pronounceable series of five lowercase letters separated by dashes. If you have reason to suspect that the public key you have received may be forged, you can for example phone the system administrator of the remote host machine and check if the fingerprint is correct.

You can save the host key on your local computer by clicking the Yes button. This is the recommended action. If you save the host key, you won't have to answer this dialog again when connecting to the same host from the same computer.

If you do not want to save the host key, click the No button. You can connect normally, but the next time you connect to the same host, the remote host will send you its public key and you will again be asked, if you want to save the key on your local computer.

You can also cancel the connection attempt by clicking the Cancel button. This results in an authentication failure, and the connection will be canceled. The host key is not saved and your local computer will not be no connected to the remote host computer.

9.2.13 Host Identification Failed

This error signifies that the identification method used by the remote host computer does not match what was expected by the SSH Secure Shell client.

A change in the host identification may be caused by one of the following reasons:

- The administrator of the remote host computer has changed the identification method.
- The administrator of the remote host computer has changed the IP address (or the host name) of the remote host.

- The administrator of the remote host computer has upgraded the system from SSH version 1 server to SSH version 2.
- An intruder is trying to pose as the remote host computer.

If you encounter this situation, do not proceed with the connection! First you should contact the system administrator of the remote host computer (preferably by phone) and check the reason for the failed identification. Only proceed with the connection when you are sure that the error is not caused by an intruder.

9.2.14 New PIN

Enter a new personal identification number (PIN) in order to continue. Enter the PIN twice, once in each field. This ensures that you have not made a typing mistake.

9.2.15 PAM Response

When using Pluggable Authentication Modules (PAM) as the authentication method, SSH Secure Shell will ask you to provide the information that the remote host computer is requesting - typically a password.

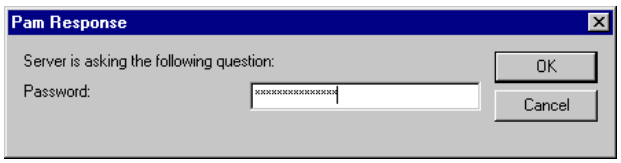

Figure 9.1: Type in your answer to the authentication query.

9.2.16 Password Needed for PFX Integrity Check

When using PKCS #12 format files to import user or CA certificates and private keys, you will have to enter the password associated with the PKCS #12 file to be imported.

9.2.17 The Remote Host Uses ssh1 Protocol

This message indicates that you are connecting to a remote host computer that is using version 1 of the Secure Shell protocol (ssh1).

Please note that an SSH version 2 (ssh2) is a more advanced protocol than the legacy version ssh1. For more information on the implications of using an ssh1 connection, see the SSH Web site (`http://www.ssh.com/products/ssh/advisories/statement.cfm`).

SSH Communications Security has deprecated the ssh1 protocol and does not recommend using it. For more information, see `http://www.ssh.com/products/ssh/advisories/deprecation.cfm`.

If you choose to accept the ssh1 connection, multiple terminal windows and the file transfer operations are not available.

If you do not want to see this message again, select the appropriate ssh1 Connections setting from the Security page of the Settings dialog. For more information on this option, see section 2.5.19 (Security).

9.2.18 Wrong Passphrase

This error indicates that the passphrase you entered is incorrect and that the private key file could not be read.

It also possible that the key file has been damaged, but this is unlikely.

This error will result in authentication failure (see section 9.2.1 (Authentication Failure)) and disconnection (see section 9.2.6 (Disconnection)). Click the OK button on both error dialogs to continue.

Try to connect again. If this error is repeated, upload your public key to the remote host computer again. For more information on this procedure, see section 3.5 (Uploading Your Public Key).

9.2.19 Wrong Password - Enter Again

This error indicates that the password you typed does not match what the remote host computer expected. You have probably made a typing mistake (or possibly left the password field blank, when the host computer expected to receive a password). Retype your password and hit the Enter key to try again.

If after several attempts you are sure that you have typed your password correctly, contact the system administrator of the remote host computer.

9.3 PKCS #11 Keys

If you have any problems with specific PKCS #11 providers, please check first for notes on your provider at `http://www.ssh.com/support/ssh/faq/`.

9.3.1 Signing error

In some cases signing errors occur when using a PKCS #11 provider key for authentication. If your PKCS #11 provider (e.g. a hardware token) has multiple keys, it may be that not all the keys can be used for authentication.

Try changing the `Slots` value in the PKCS #11 configuration (see section 2.5.14 (PKCS 11 Provider)).

When experimenting with the value, saving the settings and restarting the application, you will see different keys being used for authentication. Upload each key at a time to the remote host computer. One of the keys may be valid for authentication.

9.4 SSH1 Specific Error Messages

The following error message may be encountered when using ssh1 connection.

9.4.1 Unexpected EOF

This error message indicates that the connection to the server has been lost (literally meaning that the ssh2 client has encountered an unexpected End Of File signal).

Appendix A

Appendices

The SSH Secure Shell for Workstations Windows client is shipped with several command line tools. Their functionality is briefly explained in the following appendices. (For information on the command line options of the SSH Secure Shell for Workstations Windows client, see section 3.7 (Command Line Options).)

Also included is a list of answers to frequently asked questions about the SSH Secure Shell for Workstations Windows client.

A.1 SSH2

SSH2.EXE is a command line version of the SSH Secure Shell 2 utility.

The syntax of ssh2 is:

```
ssh2 [options] [user@]host[#port] [command]
```

The following options are available:

```
  -l user     Log in using this user name.
  +x          Enable X11 connection forwarding.
  -x          Disable X11 connection forwarding.
  -i file     Identity file for public-key authentication
  -F file     Read an alternative configuration file.
  -t          Tty; allocate a tty even if command is given.
  -v          Verbose; display verbose debugging messages.  Equal to ‘-d 2’
  -d level    Set debug level.
  -V          Display version number only.
  -q          Quiet; don’t display any warning messages.
```



```
-c cipher   Select encryption algorithm. Multiple -c options are
            allowed and a single -c flag can have only one cipher.
-m MAC      Select MAC algorithm. Multiple -m options are
            allowed and a single -m flag can have only one MAC.
-p port     Connect to this port.  Server must be on the same port.
-S          Don't request a session channel.
-L listen-port:host:port   Forward local port to remote address
-R listen-port:host:port   Forward remote port to local address
            These cause SSH to listen for connections on a port, and
            forward them to the other side by connecting to host:port.
+C          Enable compression.
-C          Disable compression.
-o 'option' Process the option as if it was read from a configuration file.
-O provider Use provider as the external key provider
-E string   Use string as initialization string for external key provider
-h          Display this help.
```

The command can be either of the following:

remote_command [arguments ...]

Run command in remote host.

-s service

Enable a service in remote server.

Type `ssh2` without arguments to see the command line syntax and the location of the configuration files.

A.2 SCP2

`SCP2.EXE` is a Windows port of the UNIX Secure Copy 2 tool (scp2).

SCP2 is used to securely copy files over the network. The program uses the ssh2 protocol for data transfer, and uses the same authentication and provides the same security as ssh2. SCP2 will ask for passwords or passphrases if they are needed for authentication.

Any file name may contain a host, user and port specification to indicate that the file is to be copied to/from that host. Copies between two remote hosts are permitted.

SCP2 uses the same host keys and user keys as the graphical SSH Secure Shell Windows client. The default location for these files is the directory used to store the user profile. The `-k` switch can be used to override the default location. Certificate authentication can be used in some configurations with SCP2, but SCP2 exists for scripting purposes and certificate usage is not recommended. (Please note that PKI and PKCS #11 support is available only in commercial distributions of the SSH Secure Shell for Workstations client.)

Please note that SCP2 offers no fallback to the ssh1 protocol.

A.2.1 SCP2 Syntax

The Windows command line version of SCP2 does not read the `ssh2_config` file or any other configuration files. It receives all its parameters from the command line.

The following parameters can be used:

```
SYNOPSIS

  scp2 [-D debug_level] [-d] [-q] [-Q] [-p] [-u] [-r] [-a] [-v] [-c cipher]
  [-C] [-P ssh2-port] [-f fw-name] [-F fw-port] [-k dir] [-V] [-h]
  [[user@]host[#port]:]file ...
  [[user@]host[#port]:]file_or_dir

OPTIONS

  -D debug_level_spec  Set debug level. (Syntax is module=level)
  -d                   Force target to be a directory.
  -q                   Make scp quiet (only fatal errors are displayed).
  -Q                   Don't show progress indicator.
  -p                   Preserve file attributes and timestamps.
  -u                   Remove source files after copying.
  -r                   Recurse subdirectories.
  -a                   transfer files in ASCII mode.
  -v                   Verbose mode; equal to '-D 2'.
  -c cipher            Select encryption algorithm. Multiple -c options are
                       allowed and a single -c flag can have only one cipher.
  -C                   Sets compression on. Default is off.
  -P ssh2-port         sshd2 port.
  -f fw-name           Firewall name.
  -F fw-port           Firewall port.
  -k dir               Store host keys and read user keys from this dir
                       instead of the user profile dir.
  -V                   Display version.
  -h                   Display this help.
```

Switches added for the Windows version of SCP2 are `-C`, `-f`, `-F` and `-k`.

A.2.2 SCP2 Return Values

The Windows command line version of SCP2 returns the following values based on the success of the operation.

```
0     Operation was successful.
1     Operation resulted in an undetermined error within sshfilecopy.
2     Destination is not directory, but it should be.
3     Maximum symlink level exceeded.
4     Connecting to host failed.
5     Connection broke for some reason.
6     File doesn't exist.
7     No permission to access file.
8     Undetermined error from sshfilexfer.
9     File transfer protocol mismatch.
```

A.3 SFTP2

`SFTP2.EXE` is a Windows port of the UNIX Secure File Transfer 2 tool (sftp2).

SFTP2 is an FTP-like client that can be used for file transfer over the network. SFTP2 uses ssh2 in data connections, so the file transport is secure.

In order to connect using SFTP2, you need to make sure that sshd2 is running on the remote host computer you are connecting to.

```
SYNOPSIS

  sftp2 [-D debug_level_spec] [-B batchfile] [-S path] [-h]
  [-V] [-P port] [-b buffer_size] [-N max_requests]
  [-c cipher] [-m mac] [user@]host[#port]


OPTIONS

  -D debug_level_spec
         Debug mode. Makes SFTP2 to send verbose debug output.
         The debugging level is either a number (0-99),
         or a comma-separated list of assignments
         ModulePattern=debug_level.

  -B batchfile
         Batch mode. Reads commands from a file instead of
```

```
        standard input. Since this mode is intended for
        scripts, SFTP2 will not try to interact with the user,
        which means that only passwordless authentication methods
        will work. In batch mode, a failure to change the current
        working directory will cause SFTP2 to abort.
        Other errors are ignored.

-S path
       Specifies the path to the ssh2 binary.

-h     Prints the command syntax and exits.

-V     Prints version information and exits.

-P port
       Specifies the port to be used.

-b buffer_size
       Specifies the size of the buffer.

-N max_requests
       Specifies the maximum number of allowed requests.

-c cipher
       Specifies the cipher to be used.

-m mac
       Specifies the MAC algorithm to be used.

 user  Specify the username to use when connecting.
       (Optional)

 host  Specify the host to connect to.

 port  Specify the port on the host to connect to.
       (Optional)
```

A.3.1 SFTP2 Commands

When SFTP2 is ready to accept commands, it will display a prompt (`sftp>`). The user can then enter any of the following commands:

open [host name]

Tries to connect to the specified host.

localopen

Opens a local connection. This is intended for debugging and testing.

close

Closes the current session.

quit

Quits the application.

cd [directory]

Changes the current remote working directory.

lcd [directory]

Changes the current local working directory.

pwd

Prints the name of the current remote working directory.

lpwd

Prints the name of the current local working directory.

ls [-R [-l] [file ...]]

Lists the names of the files on the remote server. For directories, the contents of the directory are listed.

When the -R option is specified, the directory trees are listed recursively. (By default, the subdirectories of the argument directories are not visited.)

When the -l option is specified, file sizes, modification times, permissions and owners (as supported by the file system) are also shown.

When no arguments are given, it is assumed that the contents of the current directory are being listed. Currently the options -R and - l are mutually incompatible.

lls [-R [-l] [file ...]]

The same as ls, but operates on local files.

get [file ...]

Transfers the specified files from the remote end to the local end. Directories are recursively copied with their contents.

mget [file ...]

Synonymous to get.

put [file ...]

Transfers the specified files from the local end to the remote end. Directories are recursively copied with their contents.

mput [file ...]

Synonymous to put.

rename [source [target]]

Renames the file source to target.

lrename [source [target]]

Same as rename, but operates on local files.

rm [file]

Tries to delete the specified file.

lrm [file]

The same as rm, but operates on local files.

mkdir [directory]

Tries to create the specified directory.

lmkdir [directory]

The same as mkdir, but operates on local files.

rmdir [directory]

Tries to delete the specified directory.

lrmdir [directory]

The same as rmdir, but operates on local files.

help [topic]

If topic is not given, lists the available topics. If topic is given, outputs the available online help on the topic.

A.3.2 SFTP2 Command Interpretation

SFTP2 understands both backslashes and quotation marks on the command line. A backslash can be used for ignoring the special meaning of any character in the command line interpretation. It will be removed even if the character it precedes has no special meaning.

Quotation marks can be used for specifying filenames with spaces.

Also, if you do `get .` or `put .` you will get or put every file in the current directory and possibly override files in your current directory.

SFTP2 supports wild cards (also known as glob patterns) given to commands `ls`, `lls`, `get`, and `put`.

A.4 SSH-keygen2

SSH-KEYGEN2.EXE is a Windows port of the UNIX ssh2 key generation tool (ssh-keygen2).

The ssh-keygen2 is a tool that generates and manages authentication keys for ssh2. Each user wishing to use ssh2 with public-key authentication can run this tool to create authentication keys. Additionally, the system administrator may use this to generate host keys for the SSH Secure Shell server.

(Please note that PKI and PKCS #11 support is only available in commercial distributions of SSH Secure Shell.)

SYNOPSIS

```
ssh-keygen2 [-b bits] [-t dsa|rsa] [-c comment_string]
[-e file] [-p passphrase] [-P] [-h] [-?] [-q] [-1 file] [-i]
[-D file] [-B number] [-V] [-r file] [-x file] [-k file]
[-7 file] [-F file] [key1 key2 ...]
```

OPTIONS

```
-b bits
       Length of the key in bits, for example 1024 bits.

-t dsa | rsa
       Choose the type of the key. Valid options are
       dsa and rsa.

-c comment_string
       Specify the key's comment string.

-e file
       Edit the specified key. Makes ssh-keygen2 interactive.
       You can change the key's passphrase or comment.

-p passphrase
       Specify the passphrase used.

-P     Specify that the key will be saved with an empty
       passphrase.

-h | -?
       Print a short summary of ssh-keygen2 commands.

-q     Hide the progress indicator.
```

```
-1 file
       Convert key from ssh1 format to ssh2 format.

-i file
       Load and display information on 'file'.

-D file
       Derive the public key from the private key 'file'.

-B number
       The number base for displaying key information (default 10).

-V     Print version string and exit.

-r file
       Stir in data from file to the random pool.

-x file
       Convert private key from X.509 format to ssh2 format.

-k file
       Convert a PKCS #12 file to an ssh2 format certificate
       and private key.

-7 file
       Extract certificates from a PKCS #7 file.

-F file
       Dump the fingerprint of a given publickey. The finger-
       print is given in the Bubble Babble format, which
       makes the fingerprint look like a string of "real"
       words (making it easier to pronounce).
```

A.5 Frequently Asked Questions

The FAQ gives answers to some of the most frequently asked questions about SSH Secure Shell for Workstations Windows client. For more information, see the SSH Secure Shell online FAQ (`http://www.ssh.com/faq`).

A.5.1 Connection Issues

Does SSH Secure Shell for Workstations Windows client support connecting to an ssh1 server?

Yes. But please note that this is a terminal emulation compatibility feature - this means that File Transfer, command line SCP2 and multiple windows will not work when connecting to an ssh1 server.

When connecting to a host where I know I have an account, ssh2 says `Disconnected; authentication error (No further authentication methods available.)` (for ssh-2.0.13 server), or doesn't let me in, even when I type the correct password (for newer servers). What's wrong?

The server is probably trying to check that the host name you gave it has a DNS entry. Most dialup connections do not have a DNS entry.

In older ssh2 server versions, the default `/etc/sshd2_config` file had a statement `RequireReverseMapping yes`. This should be changed to `RequireReverseMapping no`. Ask your system administrator to change this. If you still have problems, consult your system administrator.

Does the SSH Secure Shell for Workstations Windows client have support for host keys (to manage public keys of multiple hosts)?

Yes, SSH Secure Shell for Workstations Windows client supports host keys. Select the Settings option from the Edit menu, and open the Host Keys page (under Global Settings). There you can set your host keys options.

A.5.2 File Transfer Issues

I'm using SSH Secure Shell for Workstations Windows client. I can connect to the server and see the files on remote host computer, but the Modified column is blank. I would like to be able to see the last modified time.

This is a problem with the server side of the software. Most likely the server is running SSH Secure Shell server version 2.0.13 or earlier. Please ask your system administrator to update the SSH Secure Shell server software to resolve this problem.

Can I configure the SSH Secure Shell for Workstations Windows client to open the File Transfer window by default?

Yes - just open the File Transfer window, close all terminal windows and save the settings (by selecting the Save option from the File menu). The next time when you start the client, only the File Transfer window will open. When you save the settings, the window positions and types are saved so you can have any combination of windows to open by default.

A.5.3 Installation Issues

I have installed the SSH Secure Shell for Workstations Windows Client, and when I start the program, several windows are opened. What is going on?

When you save your current settings, also the window positions are saved. If you start the SSH Secure Shell client, open a new terminal window or two, and then save the settings, the 'extra' terminal windows will appear when you next time start the SSH Secure Shell client. If you open the File Transfer window and save your settings, the next time also the File Transfer window will appear.

If you have too many (or too few) windows open by default, or the window positions are not to your liking, you can always arrange the windows as you want them to appear, and then save your settings (by selecting the Save option from the File menu). The new window positions will be used when you start the SSH Secure Shell client again.

How can I uninstall the SSH Secure Shell for Workstations Windows client?

Open your Windows Control Panel (by clicking the Start button and then clicking the Control Panel option from the Settings menu). Doubleclick on the Add/Remove Programs icon, then select SSH Secure Shell, and follow the displayed instructions.

A.5.4 Licensing Issues

Do I have to reinstall if I have been using an evaluation version and purchase the software?

No, all you should need to do is import the `license.dat` file. The `license.dat` file turns an evaluation version (which is basically just the same binary without a license file) into a licensed version (either commercial or non-commercial, depending on the contents of the license file). This means that you don't necessarily need to download the binary again, if you have been evaluating the software and then decide to purchase a commercial (or non-commercial) license. This makes life easier if you have a slow Internet connection.

Use the Import License option from the Help menu to import the `license.dat` file into the SSH Secure Shell for Workstations Windows client. (Browse the directory tree to select the appropriate `license.dat` file).

A.5.5 Technical Issues

What ports does the SSH connection use?

SSH connection uses port 22 for the server, ports 1024 and higher for the client.

What type of terminal emulation is supported?

The terminal emulation is compatible up to vt320 standard (i.e. vt100, vt220, vt320, ANSI [90%]) and is partly xterm compliant.

Where can I find a list of supported platforms for SSH Secure Shell?

The list of supported platforms can be found at the SSH portability web page (`http://www.ssh.com/products/ssh/portability.html`).

A.5.6 Tunneling Issues

Can I tunnel X11 connections through Secure Shell?

Yes. Perform the following steps to forward X11 traffic:

1. Install an X emulation program (for example Exceed or Reflections).
2. Select the Settings option from the Edit menu. Select the Tunneling page on the Settings dialog. Ensure that Tunnel X11 Connections check box is checked.
3. Save your settings for the SSH Secure Shell for Workstations Windows client.
4. Logout of the SSH Secure Shell Windows client, and log back in.
5. Start the X server program.
6. Run `xterm` or `xclock` from Secure Shell, and the X11 forwarding should work.

Index

